(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3009876号
(P3009876)

(45)発行日　平成12年２月14日(2000.2.14)　(24)登録日　平成11年12月３日(1999.12.3)

(51)Int.Cl.'	識別記号	ＦＩ	
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｂ

請求項の数15(全 33 頁)

(21)出願番号　特願平10－227337
(22)出願日　平成10年８月11日(1998.8.11)
(65)公開番号　特開平11－177582
(43)公開日　平成11年７月２日(1999.7.2)
審査請求日　平成10年12月28日(1998.12.28)
(31)優先権主張番号　特願平9－228968
(32)優先日　平成９年８月12日(1997.8.12)
(33)優先権主張国　日本（ＪＰ）

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　市川　哲男
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　加山　英俊
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　山本　浩之
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100084908
弁理士　志賀　正武

審査官　萩原　義則

最終頁に続く

(54)【発明の名称】　パケット転送方法および該方法に用いる基地局

(57)【特許請求の範囲】
【請求項１】　パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮに接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、
前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に前記パケット端末の端末認証を行い、

認証に成功した前記パケット端末は、送信すべきデータを暗号化して、前記宛先端末が属するユーザＬＡＮに割り当てられる識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、
前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データを復号し、該受信パケットが改竄されていなければ、前記受信パケットに含まれる前記送信元アドレス及び前記識別子に基づいて、該識別子を持つユーザＬＡＮに対して前記パケット端末が通信を許可されている場合にだけ前記受信パケットを該ユーザＬＡＮに転送し、該通信が許可されていない場合には前記受信パケットを廃棄することを特徴とするパケット転送方法。
【請求項２】　パケット網が基地局と該基地局を接続す

るパケットバックボーン網とから構成されており．前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮに接続されているネットワークを用いたパケット通信であり．前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、

前記ユーザＬＡＮを識別する識別子を前記各ユーザＬＡＮにあらかじめ割り当てておき、

前記パケット網は、前記端末アドレスと通信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられた前記識別子と端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し．

前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に．前記情報を使用して前記パケット端末の端末認証を行い．前記パケット端末が正規の端末であれば前記パケット端末に対して通信許可を通知し．

前記パケット端末は、前記通信許可が通知されたのであれば．１つ以上の前記ユーザＬＡＮの中から通信するユーザＬＡＮを一つ選択し．送信すべきデータを暗号化して．該選択したユーザＬＡＮに割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し．

前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には．前記受信パケットに含まれる前記送信元アドレスと前記識別子との対応が前記端末情報に登録されているかどうかを確認し．該対応が登録済みである場合には前記受信パケットを前記宛先アドレスに転送し、該対応が未登録の場合には前記受信パケットを廃棄することを特徴とするパケット転送方法。

【請求項３】　パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており．前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮに接続されているネットワークを用いたパケット通信であり．前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、

前記ユーザＬＡＮ毎にあらかじめ固有のユーザＬＡＮ名を割り当てておき、

前記パケット網は、前記端末アドレスと通信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられた前記ユーザＬＡＮ名と端末認証に必要な情報を対応づけた端末情報をあらかじめ記憶し、

前記パケット端末は前記基地局を介して通信を開始する際に．１つ以上の前記ユーザＬＡＮの中から通信するユーザＬＡＮを一つ選択し．該選択したユーザＬＡＮに割り当てられた前記ユーザＬＡＮ名を前記パケット網へ通知し．

前記パケット網は、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば、前記パケット端末から通知された前記ユーザＬＡＮ名に対して前記ユーザＬＡＮを識別するための識別子を割り当てて前記パケット端末に通知し、

前記パケット端末は、送信すべきデータを暗号化して、前記選択したユーザＬＡＮに割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し．

前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には．前記受信パケットに含まれる識別子を割り当てたユーザＬＡＮ名と前記受信パケットに含まれる送信元アドレスとの対応が前記端末情報に登録されているかどうかを確認し、該対応が登録済みである場合には前記受信パケットを前記宛先アドレスに転送し．該対応が未登録の場合には前記受信パケットを廃棄し．

前記パケット網は、その後に前記パケット端末が通信を終了した時に前記ユーザＬＡＮ名に割り当てた前記識別子を解放するようにしたことを特徴とするパケット転送方法。

【請求項４】　前記パケットバックボーン網が．前記パケットを中継する複数の中継ノードを有し、これら各中継ノードが前記受信パケットを前記宛先アドレスに転送するための経路選択の機能を有するネットワークを用いたパケット転送方法であって、

前記パケット網は、前記経路選択のためのルーチング情報として前記受信パケット中の前記宛先アドレスと前記識別子とを用い．

ユニキャストパケットを転送する場合．前記宛先端末が前記パケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該パケットを前記宛先端末まで転送し．前記宛先端末が前記パケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該パケットを前記ユーザＬＡＮまで転送し、

ブロードキャストパケット及びマルチキャストパケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該パケットを順次転送し

てゆき、同じ識別子を用いて通信中の全ての前記パケット端末及び該識別子により指定される前記ユーザＬＡＮに該パケットを転送することを特徴とする請求項２記載のパケット転送方法。

【請求項５】　前記パケットバックボーン網と前記複数のユーザＬＡＮの間をゲートウェイで接続したネットワークを用いたパケット転送方法であって、

前記ユーザＬＡＮを介して前記受信パケットを前記宛先アドレスへ転送する際、前記ゲートウェイが前記受信パケットに含まれる前記識別子に応じて前記ユーザＬＡＮを選択して該選択されたユーザＬＡＮへ前記受信パケットを転送することを特徴とする請求項２～４の何れかの項記載のパケット転送方法。

【請求項６】　パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮにゲートウェイを介して接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、

前記パケット網は、前記端末アドレスと端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し、

前記ゲートウェイは、前記パケット網と前記ユーザＬＡＮの間でパケットの転送を許可する送信元の端末アドレスをあらかじめ記憶し、

前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば前記パケット端末に通信許可を通知し、

前記パケット端末は、前記通信許可が通知されたのであれば、送信すべきデータを暗号化して前記宛先アドレスと前記送信元アドレスを付与したパケットを前記パケット網へ送信し、

前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には前記受信パケットを前記ゲートウェイに転送し、

前記ゲートウェイは、前記パケット網から転送されたパケットに含まれる前記送信元アドレスに対する転送が許可されている場合は該転送パケットを前記ユーザＬＡＮから前記宛先アドレスに転送し、該転送が許可されていない場合は該転送パケットを廃棄するようにしたことを特徴とするパケット転送方法。

【請求項７】　前記パケットバックボーン網が、前記パケットを中継する複数の中継ノードを有し、これら各中継ノードが前記パケットを前記宛先アドレスに転送するための経路選択機能を有するネットワークを用いたパケット転送方法であって、

前記ユーザＬＡＮを識別する識別子を前記各ユーザＬＡＮにあらかじめ割り当てておき、

前記パケット端末は、前記パケットを前記パケット網へ送信する際に、複数の前記ユーザＬＡＮの中から接続するユーザＬＡＮを一つ選択して、該選択したユーザＬＡＮの識別子を前記パケットにさらに付与して送信し、

前記パケット網は、前記経路選択のためのルーチング情報として送信された前記パケットに含まれる前記宛先アドレスと前記識別子とを用い、

ユニキャストパケットを転送する場合、前記宛先端末が前記パケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該パケットを前記宛先端末まで転送し、前記宛先端末が前記パケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該パケットを前記ゲートウェイに転送し、

ブロードキャストパケット及びマルチキャストパケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該パケットを順次転送してゆき、同じ識別子を用いて通信中の全ての前記パケット端末と、該識別子により指定される前記ゲートウェイとに転送することを特徴とする請求項６記載のパケット転送方法。

【請求項８】　前記暗号化及び前記復号化に際し、前記ユニキャストパケットを転送する場合は、前記各パケット端末毎に割り当てた暗号鍵を用い、前記ブロードキャストパケット又は前記マルチキャストパケットを転送する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴とする請求項４又は７記載のパケット転送方法。

【請求項９】　前記暗号化及び前記復号化に際し、前記ユニキャストパケットを転送する場合及び前記パケット端末が前記ブロードキャストパケット又は前記マルチキャストパケットを送信する場合は、前記各パケット端末毎に割り当てた暗号鍵を用い、前記基地局が前記ブロードキャストパケット又は前記マルチキャストパケットを送信する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴とする請求項４又は７記載のパケット転送方法。

【請求項１０】　前記暗号化及び前記復号化に際し、暗号鍵として前記各識別子毎に割り当てた暗号鍵を用いることを特徴とする請求項４又は７記載のパケット転送方法。

【請求項１１】　他パケット網であるユーザＬＡＮが複数接続されたパケットバックボーン網に接続され、かつ、配下に複数のパケット端末を収容する基地局であっ

て．
前記各パケット端末に付与された固有の端末アドレスと．前記パケット端末が通信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられた識別子と．端末認証に必要な情報を対応づけて記憶する端末情報記憶手段と．
前記パケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行い．前記パケット端末に対して認証結果を通知する端末認証手段と．
前記パケットバックボーン網と前記パケット端末の間で授受されるパケット中のデータ部を前記情報を用いて暗号化して送信するパケット暗号化手段と、
宛先端末の前記端末アドレスである宛先アドレスと前記パケット端末の端末アドレスである送信元アドレスと前記ユーザＬＡＮに割り当てられた識別子が暗号化データに付与されたパケットを前記パケット端末から受信して該暗号化データを復号するパケット復号化手段と．
前記復号されたデータから改竄を検出して該パケットを廃棄するパケット改竄検出手段と、
前記パケットに含まれている前記送信元アドレス及び前記識別子の組が．前記端末情報記憶手段に記憶されている前記端末アドレス及び前記識別子の組の中に登録されているかどうかを確認する比較手段と．
前記比較手段による確認結果に基づいて．前記登録があることを条件に前記宛先アドレスに前記パケットを転送し．前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴とする基地局。

【請求項１２】　他パケット網であるユーザＬＡＮが複数接続されたパケットバックボーン網に接続され．かつ．配下に複数のパケット端末を収容する基地局であって．
前記各パケット端末に付与された固有の端末アドレスと．前記パケット端末が通信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられたユーザＬＡＮ名と．端末認証に必要な情報を対応づけて記憶する端末情報記憶手段と．
前記パケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行って、認証結果を前記パケット端末に通知するとともに．正規のパケット端末に対しては．前記通信開始要求に伴って前記パケット端末から通知されるユーザＬＡＮ名に前記ユーザＬＡＮを識別するための識別子を割り当てて通知し、前記パケット端末が通信を終了したことを条件として前記ユーザＬＡＮ名に割り当てた前記識別子を解放する端末認証手段と．
前記パケットバックボーン網と前記パケット端末の間で授受されるパケット中のデータ部を前記情報を用いて暗号化して送信するパケット暗号化手段と、
宛先端末の前記端末アドレスである宛先アドレスと前記パケット端末の端末アドレスである送信元アドレスと前記識別子が暗号化データに付与されたパケットを前記パケット端末から受信して該暗号化データを復号するパケット復号化手段と、
前記復号されたデータから改竄を検出して該パケットを廃棄するパケット改竄検出手段と、
前記受信したパケットに含まれる識別子を割り当てたユーザＬＡＮ名と前記受信したパケットに含まれる送信元アドレスの組が．前記端末情報記憶手段に記憶されている前記ユーザＬＡＮ名及び前記端末アドレスの組の中に登録されているかどうかを確認する比較手段と．
前記比較手段による確認結果に基づいて、前記登録があることを条件に前記宛先アドレスに前記パケットを転送し．前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴とする基地局。

【請求項１３】　前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば．前記各識別子毎に割り当てた暗号鍵を用いて暗号化し．
前記パケット復号化手段は．受信したパケットがユニキャストパケットであれば．前記各パケット端末毎に割り当てた暗号鍵を用いて復号化し、前記受信したパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて復号化することを特徴とする請求項１１記載の基地局。

【請求項１４】　前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば．前記各識別子毎に割り当てた暗号鍵を用いて暗号化し．
前記パケット復号化手段は．前記各パケット端末毎に割り当てた暗号鍵を用いて復号化することを特徴とする請求項１１記載の基地局。

【請求項１５】　前記パケット暗号化手段は、前記各識別子毎に割り当てた暗号鍵を用いて送信するパケットのデータ部を暗号化し、
前記パケット復号化手段は．前記各識別子毎に割り当てた暗号鍵を用いて受信したパケットのデータ部を復号することを特徴とする請求項１１記載の基地局。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は．無線または有線のパケット通信におけるパケット転送方法および該方法に用いる基地局に関する。さらに詳しくは、コネクションレス型のデータ通信において、パケット網に複数のＬＡＮ（Local Area Network；ローカルエリアネットワー

ク）を接続して仮想ＬＡＮ（ＶＬＡＮ）を構成したネットワークにおけるパケット転送方法および該方法に用いる基地局に関するものである。

【０００２】

【従来の技術】インターネットでは、ＩＰ（Internet Protocol；インターネットプロトコル）がパケット転送方法に採用され、このため各端末はＩＰアドレスを有する。ＩＰアドレスは３２ｂｉｔで構成され、上位ビットの一部はデータ網を識別するためのネットワークアドレスを示し、残りの下位ビットはデータ網に接続する端末を識別するためのホストアドレスを示す。

【０００３】端末は、データに宛先アドレスと送信元アドレスを付与したパケットをＩＰネットワークに送信し、ＩＰネットワークは宛先アドレス中のネットワークアドレスで示されるデータ網にパケットを転送する。データ網は、パケットがユニキャストパケットの場合は宛先アドレス中のホストアドレスで指定された端末に転送し、パケットがブロードキャストパケットの場合はデータ網に接続する全ての端末に転送する（ＲＦＣ７９１ Internet Protocol）。

【０００４】しかしながら、このようなパケット転送方法によると、送信元の端末が何者であるかを確認せずにデータ網へパケットを転送するため、未知の端末によりデータ網が不正にアクセスされる危険性がある。また、たとえ送信元端末が正規の端末であったとしても、宛先アドレスを規制していないことから、送信元端末が属するデータ網以外の他のデータ網への不正アクセスを防止できないという問題もある。

【０００５】このような不都合を解消するために、パケット転送時に宛先アドレスと送信元アドレスをチェックするパケット転送方法が提案されている。

【０００６】このアドレスチェック方法では、転送を許可する宛先アドレスと送信元アドレスとの組合せをあらかじめ許可テーブルとしてパケット転送装置に登録しておく。パケット転送装置は、転送パケットの宛先アドレスと送信元アドレスをチェックして、これらアドレスが許可テーブルに登録済みの場合は転送パケットを転送し、未登録の場合は転送パケットを転送しない（石坂 隆宏、「ネットワーク・セキュリティ装置」、特開平２－３０２１３９号公報）。

【０００７】この方法によれば、送信元アドレスを確認して、あらかじめ許可した端末アドレスの時にだけパケットを転送することにより、データ網への不正アクセスを防止している。しかし、この方法では送信元アドレスを偽造することによってデータ網へ不正にアクセスできるという問題が生じる。

【０００８】従来の他のパケット転送方法として強制転送と呼ばれる方法が提案されている。この方法は、コネクションオリエンテッド型のパケット網（即ち、Ｘ．２５に代表され、通信を開始する際にコネクションを設定するパケット網）に複数のデータ網が接続しているとき、パケット網を通してアクセスしようとする呼をパケット網がセキュリティチェック用のデータベースマシンに強制転送する。そして、データベースマシンがアクセスの正当性をチェックして、正当な場合はアクセス呼をデータ網に転送して端末－データ網間にコネクションを設定し、不当な場合はアクセス呼を切断するものである（大吉 章次、「パケット交換網におけるセキュリティチェック方式」、特開平５－３２７７７３号公報）。

【０００９】しかしながら、この方法では、パケットに付与された宛先アドレスにより転送を行うコネクションレス型のパケット網に適用した場合、セキュリティチェック用のデータベースマシンに全ての転送パケットを強制転送してアクセスの正当性をチェックする必要がある。そのために、セキュリティチェック用のデータベースマシンの負荷の増加とパケット転送遅延時間の増加という問題が生じる。

【００１０】さらに、従来の他のパケット転送方法として、不特定多数の端末が接続するインターネット等のネットワーク（以下、「中継ネットワーク」という）を経由して、リモート端末がデータ網にアクセスすることを可能にしつつ、データ網への不正アクセスを防止するカプセル化方法が提案されている。この方法では、データ網がゲートウェイを介して中継ネットワークに接続する。ゲートウェイは通信開始時にまずリモート端末の認証を行い、不正端末であることが判明した場合はパケットを破棄する。次に、リモート端末は、宛先アドレスと送信元アドレスが含まれた送信パケットを暗号化してゲートウェイへ送信する。この時、暗号化された送信パケットは、ゲートウェイ宛のパケットのデータ部に格納され、宛先データ網に接続されたゲートウェイのアドレスと送信元アドレスが付加されて中継ネットワークに転送される。なおこのようにしてパケットを転送することをカプセル化と呼んでいる。ゲートウェイは受信パケットからデータ部を取り出して暗号化されたパケットを復号する。この復号時に改竄を検出した場合はパケットを破棄し、改竄されていない場合はパケットをデータ網へ転送する。一方、データ網からリモート端末に宛てたパケットは、送信元のデータ網に接続されたゲートウェイが、宛先アドレスと送信元アドレスを付加して暗号化したのち、これに宛先アドレスと自分のゲートウェイアドレスをさらに付加し、カプセル化してリモート端末に転送する。

【００１１】この方法によれば、リモート端末を認証した後、ゲートウェイとリモート端末間にカプセル化による暗号路を設定してデータ網への不正アクセスを防止している。しかしながら、リモート端末が、中継ネットワーク経由で接続している他のリモート端末にパケットを送信する場合には、必ずゲートウェイを経由して転送されるため、最適な経路選択が行われず、パケット転送遅

遅時間が増加するという問題が生じる。また、ゲートウェイは、自身に接続しているデータ網に属する全ての端末についてカプセル化／デカプセル化処理を行う必要があり、ゲートウェイの処理負荷が増大してしまう。また、この方法では、データ網またはリモート端末がブロードキャストパケットやマルチキャストパケットを転送する場合に、中継ネットワークに送られるパケットの宛先アドレスにブロードキャストアドレスやマルチキャストアドレスを指定することができない。そのため、ゲートウェイはパケットを複製してから各リモート端末にユニキャスト転送するしかなく、中継ネットワークのトラヒック増加とパケット転送遅延時間の増加という問題が生じるほか、ゲートウェイの負荷が増大するという問題も生じる。さらに、送信元リモート端末から宛先リモート端末へユニキャストパケットを転送する場合、たとえこれらリモート端末が中継ネットワークに接続していても、必ず当該データ網に接続しているゲートウェイを経由してから宛先端末にパケットが送られるため、転送遅延時間が増加するという問題を生じる。

【００１２】

【発明が解決しようとする課題】従って本発明の第１の目的は、送信元アドレスを偽造することによりユーザＬＡＮへ不正にアクセスできてしまう問題を解決し、あらかじめ登録した端末に対してだけ特定のデータ網とのパケット転送を許可するパケット転送方法および該方法に用いる基地局を提供することにある。

【００１３】また、本発明の第２の目的は、パケットの転送遅延時間、トラヒック、ゲートウェイの負荷が増加する問題点を解決し、最適な経路選択が可能でなおかつ効率的なパケット転送方法および該方法に用いる基地局を提供することにある。

【００１４】

【課題を解決するための手段】以上の課題を解決するために、請求項１記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮに接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に前記パケット端末の端末認証を行い、認証に成功した前記パケット端末は、送信すべきデータを暗号化して、前記宛先端末が属するユーザＬＡＮに割り当てられる識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データを復号し、該受信パケットが改竄されていなければ、前記受信パケットに含まれる前記送信元アドレス及び前記識別子に基づいて、該識別子を持つユーザＬＡＮに対して前記パケット端末が通信を許可されている場合にだけ前記受信パケットを該ユーザＬＡＮに転送し、該通信が許可されていない場合には前記受信パケットを廃棄することを特徴としている。

【００１５】また、請求項２記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮに接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、前記ユーザＬＡＮを識別する識別子を前記各ユーザＬＡＮにあらかじめ割り当てておき、前記パケット網は、前記端末アドレスと通信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられた前記識別子と端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し、前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば前記パケット端末に対して通信許可を通知し、前記パケット端末は、前記通信許可が通知されたのであれば、１つ以上の前記ユーザＬＡＮの中から通信するユーザＬＡＮを一つ選択し、送信すべきデータを暗号化して、該選択したユーザＬＡＮに割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には、前記受信パケットに含まれる前記送信元アドレスと前記識別子との対応が前記端末情報に登録されているかどうかを確認し、該対応が登録済みである場合には前記受信パケットを前記宛先アドレスに転送し、該対応が未登録の場合には前記受信パケットを廃棄することを特徴としている。

【００１６】また、請求項３記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮに接続

されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、前記ユーザＬＡＮ毎にあらかじめ固有のユーザＬＡＮ名を割り当てておき、前記パケット網は、前記端末アドレスと通信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられた前記ユーザＬＡＮ名と端末認証に必要な情報を対応づけた端末情報をあらかじめ記憶し、前記パケット端末は前記基地局を介して通信を開始する際に、１つ以上の前記ユーザＬＡＮの中から通信するユーザＬＡＮを一つ選択し、該選択したユーザＬＡＮに割り当てられた前記ユーザＬＡＮ名を前記パケット網へ通知し、前記パケット網は、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば、前記パケット端末から通知された前記ユーザＬＡＮ名に対して前記ユーザＬＡＮを識別するための識別子を割り当てて前記パケット端末に通知し、前記パケット端末は、送信すべきデータを暗号化して、前記選択したユーザＬＡＮに割り当てられた識別子と前記宛先アドレスと前記送信元アドレスを該暗号化データに付与したパケットを前記パケット網へ送信し、前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には、前記受信パケットに含まれる識別子を割り当てたユーザＬＡＮ名と前記受信パケットに含まれる送信元アドレスとの対応が前記端末情報に登録されているかどうかを確認し、該対応が登録済みである場合には前記受信パケットを前記宛先アドレスに転送し、該対応が未登録の場合には前記受信パケットを廃棄し、前記パケット網は、その後に前記パケット端末が通信を終了した時に前記ユーザＬＡＮ名に割り当てた前記識別子を解放するようにしたことを特徴としている。

【００１７】また、請求項４記載の発明は、請求項２記載の発明において、前記パケットバックボーン網が、前記パケットを中継する複数の中継ノードを有し、これら各中継ノードが前記受信パケットを前記宛先アドレスに転送するための経路選択の機能を有するネットワークを用いたパケット転送方法であって、前記パケット網は、前記経路選択のためのルーチング情報として前記受信パケット中の前記宛先アドレスと前記識別子とを用い、ユニキャストパケットを転送する場合、前記宛先端末が前記パケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該パケットを前記宛先端末まで転送し、前記宛先端末が前記パケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該パケットを前記ユーザＬＡＮまで転送し、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該パケットを順次転送してゆき、同じ識別子を用いて通信中の全ての前記パケット端末及び該識別子により指定される前記ユーザＬＡＮに該パケットを転送することを特徴としている。また、請求項５記載の発明は、請求項２～４の何れかの項記載の発明において、前記パケットバックボーン網と前記複数のユーザＬＡＮの間をゲートウェイで接続したネットワークを用いたパケット転送方法であって、前記ユーザＬＡＮを介して前記受信パケットを前記宛先アドレスへ転送する際、前記ゲートウェイが前記受信パケットに含まれる前記識別子に応じて前記ユーザＬＡＮを選択して該選択されたユーザＬＡＮへ前記受信パケットを転送することを特徴としている。

【００１８】また、請求項６記載の発明は、パケット網が基地局と該基地局を接続するパケットバックボーン網とから構成されており、前記基地局が配下に複数のパケット端末を収容しており、前記パケットバックボーン網がさらに複数の他パケット網であるユーザＬＡＮにゲートウェイを介して接続されているネットワークを用いたパケット通信であり、前記各パケット端末は固有の端末アドレスを有すると共に宛先端末の前記端末アドレスである宛先アドレスと自己の端末アドレスである送信元アドレスとを付与したパケットを送信し、前記ネットワークが前記宛先アドレスを用いて前記パケットの転送を行うパケット転送方法であって、前記パケット網は、前記端末アドレスと端末認証に必要な情報とを対応づけた端末情報をあらかじめ記憶し、前記ゲートウェイは、前記パケット網と前記ユーザＬＡＮの間でパケットの転送を許可する送信元の端末アドレスをあらかじめ記憶し、前記パケット網は、前記パケット端末が前記基地局を介して通信を開始する際に、前記情報を使用して前記パケット端末の端末認証を行い、前記パケット端末が正規の端末であれば前記パケット端末に通信許可を通知し、前記パケット端末は、前記通信許可が通知されたのであれば、送信すべきデータを暗号化して前記宛先アドレスと前記送信元アドレスを付与したパケットを前記パケット網へ送信し、前記パケット網は、前記パケットを受信して該受信パケットに含まれる前記暗号化データの復号時に改竄の有無を判定し、改竄が検出されていれば前記受信パケットを廃棄し、改竄されていない場合には前記受信パケットを前記ゲートウェイに転送し、前記ゲートウェイは、前記パケット網から転送されたパケットに含まれる前記送信元アドレスに対する転送が許可されている場合は該転送パケットを前記ユーザＬＡＮから前記宛先アドレスに転送し、該転送が許可されていない場合は該転送パケットを廃棄するようにしたことを特徴としている。

【００１９】また、請求項７記載の発明は、請求項６記載の発明において、前記パケットバックボーン網が、前記パケットを中継する複数の中継ノードを有し、これら各中継ノードが前記パケットを前記宛先アドレスに転送するための経路選択機能を有するネットワークを用いたパケット転送方法であって、前記ユーザＬＡＮを識別する識別子を前記各ユーザＬＡＮにあらかじめ割り当てておき、前記パケット端末は、前記パケットを前記パケット網へ送信する際に、複数の前記ユーザＬＡＮの中から接続するユーザＬＡＮを一つ選択して、該選択したユーザＬＡＮの識別子を前記パケットにさらに付与して送信し、前記パケット網は、前記経路選択のためのルーチング情報として送信された前記パケットに含まれる前記宛先アドレスと前記識別子とを用い、ユニキャストパケットを転送する場合、前記宛先端末が前記パケット網に接続中であれば、前記宛先アドレスに応じて前記中継ノードを順次選択しながら該パケットを前記宛先端末まで転送し、前記宛先端末が前記パケット網に接続中でなければ、前記識別子に応じて前記中継ノードを順次選択しながら該パケットを前記ゲートウェイに転送し、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、前記識別子を用いて前記中継ノードを順次選択して該中継ノードに該パケットを順次転送してゆき、同じ識別子を用いて通信中の全ての前記パケット端末と、該識別子により指定される前記ゲートウェイとに転送することを特徴としている。

【００２０】また、請求項８記載の発明は、請求項４又は７記載の発明において、前記暗号化及び前記復号化に際し、前記ユニキャストパケットを転送する場合は、前記各パケット端末毎に割り当てた暗号鍵を用い、前記ブロードキャストパケット又は前記マルチキャストパケットを転送する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴としている。また、請求項９記載の発明は、請求項４又は７記載の発明において、前記暗号化及び前記復号化に際し、前記ユニキャストパケットを転送する場合及び前記パケット端末が前記ブロードキャストパケット又は前記マルチキャストパケットを送信する場合は、前記各パケット端末毎に割り当てた暗号鍵を用い、前記基地局が前記ブロードキャストパケット又は前記マルチキャストパケットを送信する場合は、前記各識別子毎に割り当てた暗号鍵を用いることを特徴としている。また、請求項１０記載の発明は、請求項４又は７記載の発明において、前記暗号化及び前記復号化に際し、暗号鍵として前記各識別子毎に割り当てた暗号鍵を用いることを特徴としている。

【００２１】また、請求項１１記載の発明は、他パケット網であるユーザＬＡＮが複数接続されたパケットバックボーン網に接続され、かつ、配下に複数のパケット端末を収容する基地局であって、前記各パケット端末に付与された固有の端末アドレスと、前記パケット端末が通

信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられた識別子と、端末認証に必要な情報を対応づけて記憶する端末情報記憶手段と、前記パケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行い、前記パケット端末に対して認証結果を通知する端末認証手段と、前記パケットバックボーン網と前記パケット端末の間で授受されるパケット中のデータ部を前記情報を用いて暗号化して送信するパケット暗号化手段と、宛先端末の前記端末アドレスである宛先アドレスと前記パケット端末の端末アドレスである送信元アドレスと前記ユーザＬＡＮに割り当てられた識別子が暗号化データに付与されたパケットを前記パケット端末から受信して該暗号化データを復号するパケット復号化手段と、前記復号されたデータから改竄を検出して該パケットを廃棄するパケット改竄検出手段と、前記パケットに含まれている前記送信元アドレス及び前記識別子の組が、前記端末情報記憶手段に記憶されている前記端末アドレス及び前記識別子の組の中に登録されているかどうかを確認する比較手段と、前記比較手段による確認結果に基づいて、前記登録があることを条件に前記宛先アドレスに前記パケットを転送し、前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴としている。

【００２２】また、請求項１２記載の発明は、他パケット網であるユーザＬＡＮが複数接続されたパケットバックボーン網に接続され、かつ、配下に複数のパケット端末を収容する基地局であって、前記各パケット端末に付与された固有の端末アドレスと、前記パケット端末が通信を許されている１つ以上のユーザＬＡＮにそれぞれ割り当てられたユーザＬＡＮ名と、端末認証に必要な情報を対応づけて記憶する端末情報記憶手段と、前記パケット端末からの通信開始要求に応じて前記情報を使用した端末認証を行って、認証結果を前記パケット端末に通知するとともに、正規のパケット端末に対しては、前記通信開始要求に伴って前記パケット端末から通知されるユーザＬＡＮ名に前記ユーザＬＡＮを識別するための識別子を割り当てて通知し、前記パケット端末が通信を終了したことを条件として前記ユーザＬＡＮ名に割り当てた前記識別子を解放する端末認証手段と、前記パケットバックボーン網と前記パケット端末の間で授受されるパケット中のデータ部を前記情報を用いて暗号化して送信するパケット暗号化手段と、宛先端末の前記端末アドレスである宛先アドレスと前記パケット端末の端末アドレスである送信元アドレスと前記識別子が暗号化データに付与されたパケットを前記パケット端末から受信して該暗号化データを復号するパケット復号化手段と、前記復号されたデータから改竄を検出して該パケットを廃棄するパケット改竄検出手段と、前記受信したパケットに含まれる識別子を割り当てたユーザＬＡＮ名と前記受信したパケットに含まれる送信元アドレスの組が、前記端末情

報記憶手段に記憶されている前記ユーザＬＡＮ名及び前記端末アドレスの組の中に登録されているかどうかを確認する比較手段と、前記比較手段による確認結果に基づいて、前記登録があることを条件に前記宛先アドレスに前記パケットを転送し、前記登録が無いことを条件に前記パケットを廃棄するフィルタリング手段とを具備することを特徴としている。

【００２３】また、請求項１３記載の発明は、請求項１１記載の発明において、前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて暗号化し、前記パケット復号化手段は、受信したパケットがユニキャストパケットであれば、前記各パケット端末毎に割り当てた暗号鍵を用いて復号化し、前記受信したパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて復号化することを特徴としている。また、請求項１４記載の発明は、請求項１１記載の発明において、前記パケット暗号化手段は、送信するパケットがユニキャストパケットであれば、各パケット端末毎に割り当てた暗号鍵を用いて暗号化し、前記送信するパケットがブロードキャストパケット又はマルチキャストパケットであれば、前記各識別子毎に割り当てた暗号鍵を用いて暗号化し、前記パケット復号化手段は、前記各パケット端末毎に割り当てた暗号鍵を用いて復号化することを特徴としている。また、請求項１５記載の発明は、請求項１１記載の発明において、前記パケット暗号化手段は、前記各識別子毎に割り当てた暗号鍵を用いて送信するパケットのデータ部を暗号化し、前記パケット復号化手段は、前記各識別子毎に割り当てた暗号鍵を用いて受信したパケットのデータ部を復号することを特徴としている。

【００２４】

【発明の実施の形態】以下、本発明の種々の実施形態について、図面を参照して説明する。なお、本発明は無線パケット網，有線パケット網の何れに対しても適用することができるが、以下では無線パケット網を中心にして説明を行い、最後に有線パケット網へ適用する場合の実施形態について説明する。

【００２５】【第１実施形態】この第１実施形態は、請求項１，２，５記載のパケット転送方法および請求項１１記載の基地局を適用した場合に相当している。

【００２６】図１は、本実施形態におけるパケット網のネットワーク構成を概略的に示している。同図において、複数の無線基地局１－６と、これら無線基地局１－６を接続する無線パケットバックボーン網１－５とで構成されるものを無線パケット網とする。各無線基地局１－６は配下に複数の無線パケット端末１－７を収容している。ユーザＬＡＮ１－４は他パケット網であって、無線パケットバックボーン網１－５はゲートウェイ１－１～１－３を介して複数のユーザＬＡＮ１－４に接続している。ゲートウェイ１－３は後述するＶＬＡＮ－ＩＤに応じて何れかのユーザＬＡＮ１－４を選択し、パケットからＶＬＡＮ－ＩＤを削除したのち、選択したユーザＬＡＮへパケットを転送する。無線パケットバックボーン網１－５とユーザＬＡＮ１－４との間の中継路１－１０としては、ＡＴＭ（Asynchronous Transfer Mode；非同期転送モード）網のバーチャルチャネルコネクション（ＶＣＣ），インターネット上のバーチャルプライベートネットワーク（ＶＰＮ）等の各種のものが選択可能である。また、無線パケットバックボーン網１－５は端末認証サーバ１－８に接続されている。この端末認証サーバ１－８は端末情報テーブルを記憶しており、無線パケット端末１－７が通信を開始する時に無線基地局１－６へ端末情報を与える。

【００２７】本実施形態において、端末情報テーブルは少なくとも端末アドレスと、後述するＶＬＡＮ－ＩＤと、端末認証に必要な情報として各端末固有の暗号鍵とを組にして持っている。端末アドレスとしてはイーサネットにおけるＭＡＣ（Media Access Control）アドレスを用いる。なお、無線パケット網はあらかじめ各無線パケット端末に暗号鍵を通知しておく。

【００２８】ここで、図２は本実施形態による無線基地局１－６の構成を示している。無線基地局１－６に設けられている各手段が有する機能については、これ以後の説明の中で順次説明してゆく。なお、同図において、実線は無線パケットバックボーン網１－５又は無線パケット端末１－７と無線基地局１－６との間で送受信されるパケット信号を意味しており、破線は無線基地局１－６内の各部間の制御信号を意味している。

【００２９】図３は、本実施形態における無線パケット端末１－７の認証手順を示している。同図に示すように、無線パケット端末１－７は通信を開始する時に通信開始要求信号を無線基地局１－６へ送信する（２－１）。無線基地局１－６では、端末認証手段１０が通信開始要求信号を受信して、端末認証サーバ１－８に端末情報要求を行う（２－２）。この端末情報要求に対して端末認証サーバ１－８が端末情報通知を無線基地局１－６に行うと、端末認証手段１０はこの端末情報通知を受けて（２－３），通知された端末情報を端末情報記憶手段１１に記憶させる。次に、端末認証手段１０は端末認証用の乱数を生成したのち、端末情報に含まれている暗号鍵を用いて暗号化し、暗号化された乱数を認証要求信号として無線パケット端末１－７に送信する（２－４）。無線パケット端末１－７は無線パケット網から通知されている暗号鍵で送信された乱数を復号化し、これを認証応答信号として無線基地局１－６に送り返す（２－５）。無線基地局１－６では、端末認証手段１０が認

証要求信号として送信した乱数と送り返された乱数を比較する。両者が一致する場合、端末認証手段１０は無線パケット端末１－７を正規端末と判断し、認証受付信号を用いて無線パケット端末１－７に通信許可を通知する（２－６）。これ以後は、パケット暗号化手段１２が端末認証手段１０から取得した暗号鍵を用いて、データパケット中のヘッダ部を除いたデータ部だけを暗号化して転送を行う。一方、上記２つの乱数が一致しない場合、端末認証手段１０は無線パケット端末１－７を不正端末と判断し、認証受付信号を用いて無線パケット端末１－７に通信拒否を通知する（２－６）。

【００３０】図４は、本実施形態におけるデータパケットの改竄検出手順を示している。無線パケット端末１－７は、生起したデータに対する誤り検出符号を計算して当該データに付与してから暗号化し、さらにヘッダ情報を付与したデータパケットを無線基地局１－６に送信する（３－１）。無線基地局１－６では、パケット復号化手段１３がデータパケット中の暗号化されたデータ部を復号してパケット改竄検出手段１４に送出する。パケット改竄検出手段１４は復号されたデータの誤り検出符号を計算し、この計算された誤り検出符号と復号によってパケットから得た誤り検出符号とを比較して、両者が一致する場合は改竄無しと判断し、両者が一致しない場合は改竄ありと判断する。

【００３１】表１は、本実施形態における端末情報テーブルを示している。端末情報テーブルは、端末アドレスと、ＶＬＡＮ－ＩＤと、端末認証に必要な情報としての暗号鍵とからなる端末情報で構成されている。なお、この端末情報は端末認証手段１０が端末情報記憶手段１１へ記憶させる（図２を参照）。

【００３２】

【表１】

第１の実施形態における端末情報テーブル

端末ｱﾄﾞﾚｽ	VLAN-ID	暗号鍵
ｱﾄﾞﾚｽ#1	VLAN-ID#A	暗号鍵#a
ｱﾄﾞﾚｽ#2	VLAN-ID#A	暗号鍵#b
ｱﾄﾞﾚｽ#3	VLAN-ID#B	暗号鍵#c

【００３３】このＶＬＡＮ－ＩＤはユーザＬＡＮ１－４を識別するための識別子として定義され、各ユーザＬＡＮに固有の値があらかじめ割り当てられている。無線パケット端末１－７は、自分の所属するユーザＬＡＮ１－４のＶＬＡＮ－ＩＤをそれぞれ端末認証サーバ１－８にあらかじめ登録している。

【００３４】図５は、本実施形態における無線パケット網が使用するパケットの信号フォーマットを示している。同図に示すように、パケットはヘッダ情報として宛先アドレス４－１，送信元アドレス４－２及びＶＬＡＮ－ＩＤ４－３を持っており、ユーザデータ４－４の部分は暗号化されている。

【００３５】以下に詳述するように、無線基地局１－６は、無線パケット端末１－７から受信したパケットの内、ＶＬＡＮ－ＩＤ４－３が当該無線パケット端末の所属するユーザＬＡＮ１－４のＶＬＡＮ－ＩＤに一致するパケットのみを転送し、これらＶＬＡＮ－ＩＤが一致しないパケットは廃棄する。

【００３６】図６は、本実施形態におけるパケット転送手順を示している。無線基地局１－６は通信開始時に図３に示した認証を行い、無線パケット端末１－７が正規端末であると判断された場合には通信を開始させる。次に、無線基地局１－６は図４に示した改竄検出手順を行い、無線パケット端末１－７から受信したデータパケット（５－１）の改竄を検出した場合はこのデータパケットを廃棄する。一方で改竄が検出されない場合、無線基地局１－６では、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５が端末情報記憶手段１１に記憶してある端末情報を参照し、ＶＬＡＮ－ＩＤと送信元アドレス４－２との対応を確認してその結果をフィルタリング手段１６に送出する。すなわち、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、表１に示す端末情報テーブルを検索して、端末アドレス、ＶＬＡＮ－ＩＤがそれぞれデータパケット中の送信元アドレス４－２，ＶＬＡＮ－ＩＤ４－３に等しいものが存在すれば、上記対応が端末情報に一致しているものと判断する。フィルタリング手段１６は送られた確認結果に基づき、上記対応が端末情報に一致していれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送する（５－２）。この時、宛先端末がユーザＬＡＮ１－４と接続していれば、データパケットはゲートウェイ１－３からゲートウェイ１－１又はゲートウェイ１－２を介してユーザＬＡＮ１－４に転送される。また、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末に転送される。一方、ＶＬＡＮ－ＩＤと送信元アドレス４－２との対応が端末情報に一致していない場合、フィルタリング手段１６はデータパケットを廃棄する。

【００３７】ここで、ユーザＬＡＮ１－４から無線パケット端末１－７へパケットを転送する場合の手順について簡単に説明しておく。ユーザＬＡＮ１－４が自身に接続しているゲートウェイ１－１又はゲートウェイ１－２にパケットを送信すると、これらゲートウェイは送信されたパケットを中継路１－１０からゲートウェイ１－３に転送する。ゲートウェイ１－３は、パケットが送られてきた中継路１－１０に応じて送信元のユーザＬＡＮ１－４に割り当てられているＶＬＡＮ－ＩＤをパケットに付与したのちに無線パケットバックボーン網１－５に転送する。無線基地局１－６は転送されてきたパケットを受信し、当該パケットのデータ部を暗号化して宛先アドレスが示す無線パケット端末１－７へ送信し、無線パケット端末１－７は暗号化されたパケットを受信して復号

する。

【００３８】以上のように，本実施形態によれば，通信開始時に端末認証することによって無線パケット端末を特定可能であり，未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止することができる。また，端末固有の暗号鍵により暗号化してパケットを転送することにより，不正な端末が認証された正規の端末になりすますことを防止可能であり，なりすまし端末による不正アクセスを防止することができる。さらに，暗号の復号時に改竄を検出してパケットを廃棄することにより，改竄されたパケットの転送を防止可能であり，改竄データによる通信の妨害と無線パケット網のトラヒック増加を防止する効果が得られる。しかも，ＶＬＡＮ－ＩＤと送信元アドレスの対応を確認することにより，認証後の端末が自分の属していないユーザＬＡＮにアクセスすることを防止可能であり，他ユーザＬＡＮに所属している端末からの不正アクセスを防止することができる。

【００３９】【第２実施形態】この第２実施形態は、請求項１，２，５記載のパケット転送方法および請求項１＊

＊１記載の基地局を適用した場合に相当している。

【００４０】本実施形態において、パケット網のネットワーク構成，無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、それぞれ図１～図５に示した第１実施形態の場合と等しい。

【００４１】第１実施形態と同様に．ＶＬＡＮ－ＩＤは各ユーザＬＡＮ１－４に固有の値があらかじめ割り当てられている。

【００４２】各無線パケット端末１－７は、接続を許可されている複数のユーザＬＡＮ１－４のＶＬＡＮ－ＩＤを端末認証サーバ１－８にあらかじめ登録している。

【００４３】表２は、本実施形態における端末情報テーブルを示している。例えば．端末アドレスとしてアドレス＃１を持つ無線パケット端末は、ＶＬＡＮ－ＩＤとしてＶＬＡＮ－ＩＤ＃Ａ又はＶＬＡＮ－ＩＤ＃Ｂを持つユーザＬＡＮ１－４に接続が許可されている。

【００４４】

【表２】

第２の実施形態における端末情報テーブル

端末ｱﾄﾞﾚｽ	VLAN-ID	VLAN-ID	暗号鍵
ｱﾄﾞﾚｽ#1	VLAN-ID#A	VLAN-ID#B	暗号鍵#a
ｱﾄﾞﾚｽ#2	VLAN-ID#A	VLAN-ID#B	暗号鍵#b
ｱﾄﾞﾚｽ#3	VLAN-ID#B	－	暗号鍵#c

【００４５】以下に詳述するように．無線基地局１－６は．無線パケット端末１－７から受信したパケットの内．当該無線パケット端末が接続を許可されているユーザＬＡＮのＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し．何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００４６】図７は、本実施形態におけるパケット転送手順を示している。無線基地局１－６では端末認証手段１０が無線パケット端末１－７に対する認証を行い、当該無線パケット端末が正規の端末であれば暗号通信を開始する。次に．無線基地局１－６ではパケット復号化手段１３が無線パケット端末１－７からのデータパケットを復号（６－１）し、パケット改竄検出手段１４は受信データパケットの改竄を調べ、改竄が検出された場合はパケットを廃棄する。なお．これまでの手順は第１実施形態と同様である。一方．改竄が検出されない場合、無線基地局１－６では、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５が端末情報記憶手段１１に記憶してある端末情報を参照し．ＶＬＡＮ－ＩＤ４－３と送信元アドレス４－２との対応が端末情報に登録済みであるかどうか確認してその結果をフィルタリング手段１６に送出する。すなわち、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は．端末情報テーブル中の端末アドレスが送信元アドレス４－２に一致し、かつ．当該端末アドレスに対応して登録されている複数のＶＬＡＮ－ＩＤの中にＶＬＡＮ－ＩＤ４－３と一致するものが存在していれば、上記対応が端末情報に登録済みであるものと判断する。そして、フィルタリング手段１６は送られた確認結果に基づいて．上記対応が端末情報に登録済みであれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送する（６－２）。この時．宛先端末がユーザＬＡＮ１－４と接続しているならば．データパケットはゲートウェイ１－３からゲートウェイ１－１又はゲートウェイ１－２を介してユーザＬＡＮ１－４に転送される。また、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末に転送される。一方．ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に未登録の場合、フィルタリング手段１６はデータパケットを廃棄する。

【００４７】以上のように．本実施形態によれば．第１実施形態から得られる効果のほかにさらに以下の効果が得られる。すなわち、ＶＬＡＮ－ＩＤと送信元アドレスの対応を確認することにより、認証後の端末が接続の許可されていないデータ網にアクセスすることを防止可能であり、接続を許可されている端末から他データ網への不正アクセスを防止することができる。また、１無線パケット端末あたり複数のＶＬＡＮ－ＩＤを登録することにより、１つの無線パケット端末で複数のデータ網にアクセスすることが可能であり、ユーザへのサービス性が向上する。

【００４８】［第３実施形態］この第３実施形態は、請求項１，２，４，５，８記載のパケット転送方法および請求項１１，１３記載の基地局を適用した場合に相当している。

【００４９】図８は、本実施形態におけるパケット網のネットワーク構成を概略的に示している。第１実施形態と同様に、無線パケット網は、複数の無線基地局７－６と、これら複数の無線基地局７－６を接続する無線パケットバックボーン網７－５とで構成されている。各無線基地局７－６はその配下に複数の無線パケット端末７－７を収容している。無線パケットバックボーン網７－５は、ゲートウェイ７－１～７－３を介して、複数のユーザＬＡＮ７－４（他パケット網）に接続されている。ここで、ゲートウェイ７－３はＶＬＡＮ－ＩＤ４－３に応じて何れかのユーザＬＡＮ７－４を選択し、パケットからＶＬＡＮ－ＩＤを削除したのち、選択したユーザＬＡＮへパケットを転送する。さらに、本実施形態における無線パケットバックボーン網７－５はパケットを中継する複数の中継ノード７－９を有している。各中継ノード７－９は、パケット中の宛先アドレス４－１及びＶＬＡＮ－ＩＤ４－３を用いたルーチング情報を有しており、このルーチング情報に従って最適な経路を選択してパケットを転送する。例えば、中継ノード７－９は、パケットを受信した時に、受信パケット中の送信元アドレス４－２が示す端末アドレスと当該パケットを受信したポート、および、受信パケット中のＶＬＡＮ－ＩＤ４－３と当該パケットを受信したポートを対応づけて記憶する。次に、中継ノード７－９は、受信パケットがユニキャストパケットならば、宛先アドレス４－１が示す端末アドレスに対応するポートへ受信パケットを送信する。これに対し、受信パケットがブロードキャストパケット又はマルチキャストパケットならば、中継ノード７－９はＶＬＡＮ－ＩＤ４－３に対応する全てのポートへ受信パケットを送信する。なお、ここで言う"ポート"は、中継ノード７－９が自身に隣接する中継ノード又は無線基地局との間の通信路を接続するためのインタフェースである。また、中継路７－１０としては、図１に示した中継路１－１０と同様に各種のものが選択可能である。また、無線パケットバックボーン網７－５は中継ノード７－９を介して端末認証サーバ７－８に接続されている。端末認証サーバ７－８は図１に示した端末認証サーバ１－８と同じく表２に示した端末情報テーブルを記憶しており、無線パケット端末７－７が通信を開始する際に無線基地局７－６に対して端末情報を与える。

【００５０】本実施形態において、この端末情報テーブルに登録された暗号鍵は端末認証及びユニキャストパケットの暗号化に用いられ、以下ではこの暗号鍵を「端末鍵」という。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【００５１】以上に加えて、端末認証サーバ７－８は表３に示すＶＬＡＮ情報テーブルにＶＬＡＮ情報を持っている。

【００５２】

【表３】

第３の実施形態におけるVLAN情報テーブル

VLAN-ID	VLAN鍵
VLAN-ID#A	VLAN鍵#a
VLAN-ID#B	VLAN鍵#b

【００５３】このＶＬＡＮ情報テーブルは、ＶＬＡＮ－ＩＤと、同じＶＬＡＮ－ＩＤを持つ全ての端末で共通に使用する暗号鍵（以下、「ＶＬＡＮ鍵」という）との対応を記録している。このＶＬＡＮ鍵はブロードキャストパケット及びマルチキャストパケットの暗号化に使用される。なお、無線パケット網は各無線パケット端末７－７に対してＶＬＡＮ鍵をあらかじめ通知しておく。

【００５４】第１実施形態と同様に、ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【００５５】無線パケット端末７－７は自分の所属するユーザＬＡＮ７－４のＶＬＡＮ－ＩＤをそれぞれ端末認証サーバ７－８の端末情報テーブルにあらかじめ登録している。

【００５６】以下に詳述するように、無線基地局７－６は、無線パケット端末７－７から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザＬＡＮ７－４のＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し、何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００５７】本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【００５８】図９は、本実施形態におけるパケット転送手順を示している。第１実施形態と同様に、無線基地局７－６では、端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い、当該無線パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して、端末認証手段１０は端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得て端末情報記憶手段１１に記憶させる。一方、無線パケット端末７－７は、ユニキャストパケットを送信する時には端末鍵を選択して暗号化を行い、暗号化されたデータパケットを無線基地局７－６に送信する（８－１）。一方、無線パケット端末７－７は、ブロードキャストパケット又はマルチキャストパケットを送信する時にはＶＬＡＮ鍵を選択して暗号化を行い、暗号化されたデータパケットを無線基地局７－６に送信する（８－１）。これらに対応して、無線基地局７－６のパケット復号化手段１３は、ユニキャストパケットを受信した時には端末鍵を選択し

てデータパケットを復号し．また、ブロードキャストパケット又はマルチキャストパケットを受信した時にはＶＬＡＮ鍵を選択してデータパケットを復号する。パケット改竄検出手段１４は、図４に示した改竄検出手順に従って復号されたデータパケットの改竄の有無を調べ、改竄が検出された場合にはデータパケットを廃棄する。一方．データパケットの改竄が検出されない場合．端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、第２実施形態と同様にしてＶＬＡＮ－ＩＤ４－３と送信元アドレス４－２の対応を確認し、これらの対応が端末情報に登録済みであれば宛先アドレスで指定された宛先端末にデータパケットを転送する（８－２）。この時、本実施形態では．宛先端末がユーザＬＡＮ７－４と接続している場合．各中継ノード７－９はデータパケット中の宛先アドレス４－１に応じて次の送信ポートを選択してゲートウェイ７－３へデータパケットを転送する。ゲートウェイ７－３はＶＬＡＮ－ＩＤ４－３に応じてゲートウェイ７－１又はゲートウェイ７－２の何れかを選択してデータパケットをユーザＬＡＮ７－４に転送する。また．宛先端末が無線パケット網と接続している場合、各中継ノード７－９は宛先アドレス４－１に応じて次の送信ポートを選択してデータパケットを宛先端末へ転送する。したがってこの場合はゲートウェイを介することなくデータパケットが転送される。一方、ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段１６はデータパケットを廃棄する。

【００５９】図１０は、本実施形態におけるブロードキャストパケットの転送手順を示している。送信元端末ではデータが生起するとブロードキャストパケットを無線基地局７－６に送信する（９－１）．無線基地局７－６では．パケット暗号化手段１２が端末認証手段１０から取得した暗号鍵のうちＶＬＡＮ鍵を選択（９－２）してブロードキャストパケットを暗号化（９－３）し．全てのパケット端末（同図では無線パケット端末＃１．＃２）へブロードキャストパケットを送信する（９－４）。各無線パケット端末＃１，＃２では、暗号鍵としてＶＬＡＮ鍵を選択（９－５）し、暗号化されたブロードキャストパケットを復号化する（９－６）。このように本実施形態では、暗号化にＶＬＡＮ鍵を用いているため．同じＶＬＡＮ－ＩＤを有するパケット端末がブロードキャストパケット及びマルチキャストパケットを復号化することが可能である。

【００６０】図１１は、ブロードキャストパケットがネットワーク内を転送されてゆく様子を示している。同図に示すように．ユーザＬＡＮ＃Ａに属する無線パケット端末７－７ａ（送信端末）がブロードキャストパケットを無線基地局７－６ａに送信すると．このパケットは無線パケットバックボーン網７－５に送出される。無線パケットバックボーン網７－５は、ＶＬＡＮ－ＩＤ４－３に応じて中継ノード７－９ａからゲートウェイ７－３及び中継ノード７－９ｂにブロードキャストパケットを転送する。ここで．ゲートウェイ７－３はＶＬＡＮ－ＩＤ４－３を見て．ユーザＬＡＮ＃Ａに接続されたゲートウェイ７－１へブロードキャストパケットを転送する。一方．中継ノード７－９ｂはブロードキャストパケットをさらに中継ノード７－９ｃと転送し．中継ノード７－９ｃは．ユーザＬＡＮ＃Ａに属する無線パケット端末７－７ｃが接続された無線基地局７－６ｃにブロードキャストパケットを転送する。

【００６１】このように．ＶＬＡＮ－ＩＤを用いたルーチング情報によって経路が選択されてブロードキャストパケットが転送される。また、無線基地局７－６ｂにはユーザＬＡＮ＃Ｂに属する無線パケット端末７－７ｂのみが接続されており、ＶＬＡＮ－ＩＤ４－３と同じＶＬＡＮ－ＩＤを有する無線パケット端末を配下に持っていない。したがって、中継ノード７－９ｂは無線基地局７－６ｂに対してブロードキャストパケットを転送しない。

【００６２】なお、上述した説明では第２実施形態を基にしたパケット転送手順について説明したが、第１実施形態を基にしても良い。そうした場合．端末情報テーブルとしては表２の代わりに表１を使用することになるほか．ＶＬＡＮ－ＩＤと送信元アドレスの対応が端末情報に登録済みであるか確認する（図９における８－３）代わりに、この対応が端末情報に一致するかどうか確認することになる（図６における５－３）。

【００６３】以上のように．本実施形態によれば第１～第２実施形態に加えて以下の効果が得られる。すなわち．本実施形態では、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には．ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【００６４】また、ブロードキャストパケット又はマルチキャストパケットを転送する場合は．ＶＬＡＮ－ＩＤに応じて次の中継ノードを選択して転送するため．同じＶＬＡＮ－ＩＤを用いて通信している全ての無線パケット端末に対してゲートウェイからユニキャスト転送する必要がない。したがって．最適な経路選択でパケットを転送することが可能であり．転送遅延時間，トラヒック．ゲートウェイの処理負荷の増加をそれぞれ防止することができる。

【００６５】また、ＶＬＡＮ－ＩＤが同じであれば共通の暗号鍵を用いてブロードキャストパケット又はマルチキャストパケットを暗号化しているため、無線基地局は．同一のＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して．１回の送信でブロードキャストパケット又はマルチキャストパケットを転送することが可能となる。したがって．各無線パケット端末の暗号鍵を用いて

暗号化したパケットを復数回送信する場合に比べて、トラヒック，転送遅延時間，基地局の負荷を抑制することができる。なお，ＶＬＡＮ鍵は端末固有の暗号鍵ではないが，異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【００６６】【第４実施形態】この第４実施形態は、請求項１，２，４，５，９記載のパケット転送方法および請求項１１，１４記載の基地局を適用した場合に相当している。

【００６７】本実施形態におけるパケット網のネットワーク構成は図８に示した第３実施形態の構成に等しい。また，本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【００６８】第３実施形態と同様に，ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【００６９】無線パケット端末７－７は、自分の所属するユーザＬＡＮ７－４のＶＬＡＮ－ＩＤをあらかじめ端末認証サーバ７－８の端末情報テーブルに登録している。

【００７０】第３実施形態と同様に，無線基地局７－６は，無線パケット端末７－７から受信したパケットの内，当該無線パケット端末が接続を許可されているユーザＬＡＮ７－４のＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し、何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００７１】また，端末認証サーバ７－８は表３に示した第３実施形態と同じＶＬＡＮ情報テーブルを持っており，ＶＬＡＮ鍵はブロードキャストパケット及びマルチキャストパケットの暗号化に使用される、無線パケット網が各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておくことも第３実施形態と同じである。

【００７２】本実施形態における端末情報テーブルは表２に示した第２実施形態の端末情報テーブルと等しい。この端末情報テーブルに登録された暗号鍵（端末鍵）は，端末認証時，ユニキャストパケットの暗号化時，ならびに，無線パケット端末によるブロードキャスト及びマルチキャストパケットの暗号化時にそれぞれ用いられる。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【００７３】図１２は、本実施形態におけるパケット転送手順を示している。無線基地局７－６では、第３実施形態と同様にして，端末認証手段１０が通信開始時において無線パケット端末７－７に対する認証を行い，当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に，第３実施形態とは異なって、無線パケット端末７－７はユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく端末鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１１－１）。無線基地局７－６では、パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなく端末鍵を用いてデータパケットを復号化する。そしてこれ以後の手順は第３実施形態と同じである。無線基地局７－６は、受信したデータパケットが改竄されていればデータパケットを廃棄し，改竄されていなければＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録済みであれば宛先アドレス４－１で指定される宛先端末にデータパケットを転送する（１１－２）。このとき、データパケットは第３実施形態と同様に転送されてゆく。一方，ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録されていない場合，フィルタリング手段１６はデータパケットを廃棄する。

【００７４】本実施形態では、無線基地局７－６が送信するブロードキャストパケット及びマルチキャストパケットの暗号化の際には第３実施形態と同様にＶＬＡＮ鍵を用いるため，同じＶＬＡＮ－ＩＤを有するパケット端末はブロードキャストパケット及びマルチキャストパケットの復号が可能である。一方、無線パケット端末７－７が送信するブロードキャストパケット及びマルチキャストパケットの暗号化には端末鍵を用いているため、無線基地局７－６は第３実施形態のように２種類の暗号鍵（端末鍵，ＶＬＡＮ鍵）を切り替えて暗号を復号化する必要がない。

【００７５】また、本実施形態においてブロードキャストパケットをパケット網で転送する様子は、図１０～図１１に示す第３実施形態の場合に等しい。すなわち、無線基地局７－６がブロードキャスト又はマルチキャストパケットを送信する場合には、ＶＬＡＮ鍵を用いてパケットの暗号化が行われることになる。

【００７６】なお、上述した説明では第２実施形態を基にしたパケット転送手順について説明したが、第１実施形態を基にしても良い。その場合には，第３実施形態で説明したように，表１に示す端末情報テーブルを使用するとともに、ＶＬＡＮ－ＩＤと送信元アドレスの対応が端末情報に一致するかどうか確認することになる。

【００７７】以上のように，本実施形態によれば，第３実施形態と同様に、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【００７８】これに加えて本実施形態では、無線基地局がブロードキャストパケット又はマルチキャストパケッ

トを転送する際には、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化している。このため、無線基地局は同じＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して１回の送信でパケット転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。

【００７９】また、無線パケット端末がブロードキャストパケット又はマルチキャストパケットを転送する際、ユニキャストパケット用の暗号鍵を用いて暗号化している。したがって、無線基地局は無線パケット端末からパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となり、ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて、無線基地局にかかる負荷を抑制することができる。

【００８０】【第５実施形態】この第５実施形態は、請求項１，２，４，５，１０記載のパケット転送方法および請求項１１，１５記載の基地局を適用した場合に相当している。

【００８１】本実施形態におけるパケット網のネットワーク構成は、図８に示す第３実施形態の構成に等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【００８２】第３実施形態と同様に、ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【００８３】端末認証サーバ７－８は第３実施形態と同様に端末情報テーブル及びＶＬＡＮ情報テーブルを有している。

【００８４】第３実施形態と同様に、無線基地局７－６は、無線パケット端末７－７から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザＬＡＮ７－４のＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し、何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００８５】本実施形態では、ＶＬＡＮ鍵はパケットを暗号化するときに使用される。なお、無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【００８６】本実施形態における端末情報テーブルは、表２に示した第２実施形態の端末情報テーブルと等しい。ここで、本実施形態ではこの端末情報テーブルに登録する暗号鍵として、各パケット端末が所属するユーザＬＡＮ７－４のＶＬＡＮ鍵を用いる。

【００８７】図１３は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、第３実施形態及び第４実施形態とは異なって、無線パケット端末７－７はユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なくＶＬＡＮ鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１２－１）。無線基地局７－６では、パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなくＶＬＡＮ鍵を用いてデータパケットを復号化する。そしてこれ以後の手順は第３実施形態と同じである。無線基地局７－６は、受信したデータパケットが改竄されていればパケットを廃棄し、改竄されていなければＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録済みであれば宛先アドレス４－１で指定される宛先端末にデータパケットを転送する（１２－２）。このとき、データパケットは第３実施形態と同様に転送されてゆく。一方、ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段１６はデータパケットを廃棄する。

【００８８】本実施形態では、第３実施形態と違って暗号化にＶＬＡＮ鍵のみを用いるようにして端末鍵を用いてないため、同じＶＬＡＮ－ＩＤを有する無線パケット端末が、ブロードキャストパケット及びマルチキャストパケットに施された暗号を復号化することが可能である。また、無線基地局及び無線パケット端末は２種類の暗号鍵を切り替えて暗号化及び復号化を行う必要がないため、無線基地局及び無線パケット端末にかかる負荷を抑制することができる。

【００８９】なお、本実施形態においてブロードキャストパケットをパケット網で転送する様子は、図１１に示す第３実施形態の場合に等しい。また、上述した説明では第２実施形態を基にしたパケット転送手順について説明したが、第１実施形態を基にしても良い。その場合には、第３実施形態で説明したように、表１に示す端末情報テーブルを使用するとともに、ＶＬＡＮ－ＩＤと送信元アドレスの対応が端末情報に一致するかどうか確認することになる。

【００９０】以上のように、本実施形態によれば、第３実施形態と同様に、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【００９１】これに加えて本実施形態では、パケットを転送する際、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため、無線基地局は同じＶＬＡＮ－ＩＤを有する配下の全無線パケット端末に対して、１回の送

信でブロードキャストパケット及びマルチキャストパケットを転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。

【００９２】また、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いているため、無線基地局及び無線パケット端末はパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となる。したがって、２種類の暗号鍵を用いる場合に比べて、無線基地局及び無線パケット端末にかかる負荷を抑制することができる。なお、ＶＬＡＮ鍵は端末固有の暗号鍵ではないが、異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【００９３】〔第６実施形態〕この第６実施形態は、請求項１，３，５記載のパケット転送方法および請求項１２記載の基地局を適用した場合に相当している。本実施形態では第１実施形態に変形を加えて、ＶＬＡＮ－ＩＤを通信開始時において動的に割り当てるようにしたものである。本実施形態におけるパケット網のネットワーク構成、無線基地局の構成、データパケットの改竄検出手順及びパケットの信号フォーマットは、図１，図２，図４及び図５に示した第１実施形態の場合とそれぞれ等しい。

【００９４】本実施形態では、ＶＬＡＮ－ＩＤの動的割り当てを実現するためにユーザＬＡＮ１－４の各々にあらかじめ固有の名称（以下、「ユーザＬＡＮ名」という）を割り当てておく。例えば図１において、ＬＡＮ＃Ａには「ユーザＬＡＮ＃Ａ」を割り当て、ＬＡＮ＃Ｂには「ユーザＬＡＮ＃Ｂ」を割り当てるようにする。また、本実施形態ではユーザＬＡＮ名とＶＬＡＮ－ＩＤの対応関係を保持するために、無線基地局１－６が表４に示すＶＬＡＮ－ＩＤ割当管理テーブルを記憶している。さらに本実施形態において、端末認証サーバ１－８の保持する端末情報テーブルは表５に示す通りであり、ＶＬＡＮ－ＩＤの代わりにユーザＬＡＮ名を使用する点が第１実施形態（表１）と異なっている。

【００９５】

【表４】

VLAN-ID割当管理テーブル

ユーザLAN名	VLAN-ID
ユーザLAN#A	VLAN-ID#A
ユーザLAN#B	VLAN-ID#B
⋮	⋮

【００９６】

【表５】

端末情報テーブル

端末アドレス	ユーザLAN名	暗号鍵
アドレス#1	ユーザLAN#A	暗号鍵#a
アドレス#2	ユーザLAN#A	暗号鍵#b
アドレス#3	ユーザLAN#B	暗号鍵#c

【００９７】本実施形態では図３に示した認証手順に一部変更を加えて図１４に示す無線パケット端末の認証手順を採用している。図１４に示すように、無線パケット端末１－７は通信開始要求信号を無線基地局１－６へ送信する際に、自分の所属しているユーザＬＡＮに割り当てられたユーザＬＡＮ名（例えば「ユーザＬＡＮ＃Ａ」）を含めて送信している（１８－１）。無線基地局１－６では、端末認証手段１０が送られたユーザＬＡＮ名を内部に記憶しておく。次に、第１実施形態と同様に、無線基地局１－６は端末認証サーバ１－８に要求（２－２）を行って端末情報を取得（２－３）してこれを端末情報記憶手段１１に記憶し、端末認証用の乱数を暗号化して無線パケット端末１－７に認証要求信号を送信（２－４）し、無線パケット端末１－７が送り返す認証応答信号（２－５）に基づいて認証を行う。

【００９８】この認証によって無線パケット端末１－７が正規の端末と判断された場合、端末認証手段１０は無線パケット端末１－７から通知（１８－１）されているユーザＬＡＮ名にＶＬＡＮ－ＩＤを割り当てる（１８－６）。いま、無線パケット端末１－７から通知された例えばユーザＬＡＮ名が「ユーザＬＡＮ＃Ａ」である場合、端末認証手段１０はこのユーザＬＡＮに対して例えば「ＶＬＡＮ－ＩＤ＃Ａ」を割り当て、表４に示すように「ユーザＬＡＮ＃Ａ」および「ＶＬＡＮ－ＩＤ＃Ａ」の組をＶＬＡＮ－ＩＤ割当管理テーブルに追加する。次いで、端末認証手段１０は認証受付信号を用いて無線パケット端末１－７に通信許可を通知するが、このとき端末認証手段１０はいま割り当てたＶＬＡＮ－ＩＤ＃Ａを無線パケット端末１－７に通知する（１８－７）。なお、無線パケット端末１－７が不正端末と判断された場合の処理は第１実施形態と同じである。

【００９９】一方、図１５は本実施形態におけるパケット転送手順を示している。まず、本実施形態では認証手順として図１４に示した認証手順を実行する（１９－１）。次に、無線パケット端末１－７はデータパケットを無線基地局１－６に送信するが、その際、ＶＬＡＮ－ＩＤ４－３としては先に通知されたＶＬＡＮ－ＩＤ（図１４の１８－７）を用いる。この後は、第１実施形態と同様にして宛先端末へのデータパケットの転送（５－２）の処理までを行うが、データパケットが改竄されておらず、ユーザＬＡＮ名と送信元アドレスの対応が端末情報に一致するかどうか確認する際（１９－２）には次に述べる処理を行う。すなわち、無線基地局１－６では、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５が、送

信元アドレス４－２に対応するユーザＬＡＮ名を表５に示す端末情報テーブルから取得し、取得したユーザＬＡＮ名に対応するＶＬＡＮ－ＩＤを表４に示すＶＬＡＮ－ＩＤ割当管理テーブルから検索し、検索されたＶＬＡＮ－ＩＤとデータパケット中のＶＬＡＮ－ＩＤ４－３が一致するかどうか判定する。フィルタリング手段１６はこの判定結果に基づいて、両者が一致していれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送（５－２）し、両者が一致していなければデータパケットを廃棄する。その後に、無線パケット端末１－７と宛先端末との間で通信が終了したならば、無線基地局１－６では端末認証手段１０が表４に示したＶＬＡＮ－ＩＤ割当管理テーブルから「ユーザＬＡＮ#Ａ」および「ＶＬＡＮ－ＩＤ#Ａ」の組を削除しそれによって、無線パケット端末１－７に割り当てたＶＬＡＮ－ＩＤを解放する（１９－３）。

【０１００】以上のように、本実施形態では無線パケット端末１－７に対してＶＬＡＮ－ＩＤを動的に割り当てているため、限られたＶＬＡＮ－ＩＤを効率的に再利用＊

＊することができ、より多くのユーザＬＡＮを収容することができる。

【０１０１】【第７実施形態】この第７実施形態は、請求項１，３，５記載のパケット転送方法および請求項１２記載の基地局を適用した場合に相当している。本実施形態は、第６実施形態で説明したＶＬＡＮ－ＩＤの動的割り当てを第２実施形態に適用したものである。したがって、本実施形態におけるパケット網のネットワーク構成、無線基地局の構成，データパケットの改竄検出手順及びパケットの信号フォーマットは、図１，図２，図４及び図５に示した第１実施形態の場合とそれぞれ等しい。

【０１０２】本実施形態では、端末認証サーバ１－８が表６に示す端末情報テーブルを記憶している。表５（第６実施形態）と比較した場合、一つの端末アドレスについて、当該端末アドレスを持つパケット端末に通信を許可するユーザＬＡＮ名が複数登録されている。

【０１０３】

【表６】

端末情報テーブル

端末アドレス	ユーザLAN名	ユーザLAN名	暗号鍵
アドレス#1	ユーザLAN#A	ユーザLAN#B	暗号鍵#a
アドレス#2	ユーザLAN#A	ユーザLAN#B	暗号鍵#b
アドレス#3	ユーザLAN#B	-	暗号鍵#c

【０１０４】本実施形態における無線パケット端末の認証手順は図１６に示すものとなる。図１６に示す認証手順と図１４（第６実施形態）との相違は、無線パケット端末１－７が通信開始要求信号を無線基地局１－６へ送信する際に、通信相手のユーザＬＡＮ名を指定して無線基地局１－６に通知する（２０－１）点である。したがって、この後に行われる認証手順は第６実施形態と同じである。

【０１０５】一方、図１７は本実施形態におけるパケット転送手順を示している。本実施形態では、まず認証手順として図１６に示した手順を実行する（２１－１）。次に、無線パケット端末１－７はデータパケットを無線基地局１－６に送信するが、その際、ＶＬＡＮ－ＩＤ４－３としては先に通知されたＶＬＡＮ－ＩＤ（図１６の１８－７）を用いる。この後は、第２実施形態と同様にして宛先端末へのデータパケットの転送（６－２）の処理までを行うが、データパケットが改竄されておらず、ユーザＬＡＮ名と送信元アドレスの対応が端末情報に登録済みかどうか確認する際（２１－２）には次に述べる処理を行う。すなわち、無線基地局１－６において、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信パケットに含まれるＶＬＡＮ－ＩＤ４－３に対応するユーザＬＡＮ名を表４に示すＶＬＡＮ－ＩＤ割当管理テーブルから検索し、検索されたユーザＬＡＮ名と受信パケットに含まれる送信元アドレス４－２の組が、表６に示す端末情報テーブル中の端末アドレスとユーザＬＡＮ名の複数の組の中に存在するかどうかを調べ、この組が端末情報テーブルに存在していなければ上記対応が端末情報に未登録であると判断する。一方、この組が端末情報テーブルに存在する場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は当該ユーザＬＡＮ名に割り当ててあるＶＬＡＮ－ＩＤを表４に示すＶＬＡＮ－ＩＤ割当管理テーブルから取得し、取得したＶＬＡＮ－ＩＤとパケット中のＶＬＡＮ－ＩＤ４－３が一致するかどうか調べ、一致していれば上記対応が端末情報に登録済みであると判断し、一致していなければ上記対応が端末情報に未登録であると判断する。フィルタリング手段１６は、この判断結果に基づいて上記対応が端末情報に登録済みであれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送（６－２）し、上記対応が端末情報に未登録であればデータパケットを廃棄する。その後、無線パケット端末１－７と宛先端末の間で通信が終了したならば、第６実施形態と同様にして、端末認証手段１０は無線パケット端末１－７に割り当てたＶＬＡＮ－ＩＤを解放する（２１－３）。

【０１０６】【第８実施形態】この第８実施形態は、請求項１，２，５記載のパケット転送方法および請求項１１記載の基地局を適用した場合に相当している。これまで説明した各実施形態では、端末アドレスとしてＭＡＣアドレスを用い、ユーザＬＡＮに対してＶＬＡＮ－ＩＤ

を割り当てるようにしていた。これに対して、本実施形態では端末アドレスとしてＩＰアドレスを用いるとともに、ユーザＬＡＮには各ユーザＬＡＮ１－４に対して固有のネットワークアドレスをあらかじめ割り当てておく。前述したようにＩＰアドレスは図１８に示す構成をしているが、本実施形態ではこのＩＰアドレスに含まれるネットワークアドレス部をＶＬＡＮ－ＩＤの代わりに用いる。つまり、本実施形態においてはデータパケット中の宛先アドレス４－１の上位ビットを抽出することでネットワークアドレスが得られることになる。したがって、図５に示したＶＬＡＮ－ＩＤ４－３は不要となり、本実施形態における信号フォーマットは図１９に示すものとなる。

【０１０７】また、本実施形態における端末情報テーブルは表７に示すものとなり、表１で使用されていたＶＬＡＮ－ＩＤの代わりにネットワークアドレスが使用される。さらに、本実施形態における無線パケット端末１－７は、自分の所属するユーザＬＡＮ１－４のネットワークアドレスをそれぞれ端末認証サーバ１－８にあらかじめ登録している。なお、本実施形態におけるパケット網のネットワーク構成，，無線基地局の構成，無線パケット端末の認証手順及びデータパケットの改竄検出手順は、図１～図４に示した第１実施形態の場合とそれぞれ等しい。

【０１０８】

【表７】

端末情報テーブル

端末アドレス	ネットワークアドレス	暗号鍵
アドレス#1	ネットワークアドレス#A	暗号鍵#a
アドレス#2	ネットワークアドレス#A	暗号鍵#b
アドレス#3	ネットワークアドレス#B	暗号鍵#c

【０１０９】図２０は本実施形態におけるパケット転送手順を示しており、図６（第１実施形態）に示したパケット転送手順とは以下の点が相違する。すなわち、無線＊基地局１－６では、パケット改竄検出手段１４が受信したデータパケット（５－１）の改竄を検出しなかった場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信したデータパケットの宛先アドレス４－１からネットワークアドレス部を抽出し、送信元アドレス４－２に基づいて表７に示した端末情報テーブルから無線パケット端末１－７の所属するユーザＬＡＮのネットワークアドレスを取得して、これら２つのネットワークアドレスが一致するかどうかを確認する（２４－１）。その後、フィルタリング手段１６は送られた確認結果に基づいて、両ネットワークアドレスが一致していれば第１実施形態と同様に宛先アドレス４－１で指定された宛先端末にデータパケットを転送する（５－２）。一方、両ネットワークアドレスが一致していなければ、フィルタリング手段１６はデータパケットを廃棄する。

【０１１０】以上のように、本実施形態では、第１実施形態のようにデータパケット中にＶＬＡＮ－ＩＤのような余分なフィールドを設ける必要がない。

【０１１１】［第９実施形態］この第９実施形態は、請求項１，２，５記載のパケット転送方法および請求項１１記載の基地局を適用した場合に相当している。本実施形態は、第８実施形態で説明したネットワークアドレスの使用を第２実施形態に適用したものである。本実施形態においても、ユーザＬＡＮ１－４に対して各ユーザＬＡＮに固有のネットワークアドレスをあらかじめ割り当てておく。また、本実施形態における端末情報テーブルは表８に示す通りであって、表２で使用されていたＶＬＡＮ－ＩＤの代わりにネットワークアドレスが使用されている。なお、本実施形態におけるパケット網のネットワーク構成，無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図１～図４及び図１９に示したものとそれぞれ等しい。

【０１１２】

【表８】

＊端末情報テーブル

端末アドレス	ネットワークアドレス	ネットワークアドレス	暗号鍵
アドレス#1	ネットワークアドレス#A	ネットワークアドレス#B	暗号鍵#a
アドレス#2	ネットワークアドレス#A	ネットワークアドレス#B	暗号鍵#b
アドレス#3	ネットワークアドレス#B	－	暗号鍵#c

【０１１３】図２１は本実施形態におけるパケット転送手順を示しており、図７（第２実施形態）に示したパケット転送手順とは以下の点が相違する。すなわち、無線基地局１－６では、パケット改竄検出手段１４が受信したデータパケット（６－１）の改竄を検出しなかった場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信したデータパケットの宛先アドレス４－１からネットワークアドレス部を抽出し、送信元アドレス４－２に基づいて無線パケット端末１－７が通信を許されているユーザＬＡＮに割り当てられている全てのネットワークアドレスを表８に示した端末情報テーブルから取得する。次いで、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、取得したネットワークアドレスの中に宛先アドレス４－１から抽出されたネットワークアドレスと一致するものが登録されているかどうか確認する。フィルタリング手段１６は送られた確認結果に基づいて、一致するネ

ットワークアドレスが存在していれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送（６－２）し、一致するネットワークが全く無ければデータパケットを廃棄する。

【０１１４】以上のように、本実施形態においても、第１実施形態のようにデータパケット中にＶＬＡＮ－ＩＤのような余分なフィールドを設ける必要がない。

【０１１５】【第１０実施形態】この第１０実施形態は、請求項１、２、４、５、８記載のパケット転送方法および請求項１１、１３記載の基地局を適用した場合に相当している。本実施形態は、第８実施形態で説明したネットワークアドレスの使用を第３実施形態に適用したものである。本実施形態においても、ユーザＬＡＮ１－４には各ユーザＬＡＮに固有のネットワークアドレスをあらかじめ割り当てておく。本実施形態におけるパケット網のネットワーク構成は図８に示した第３実施形態の場合と等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図４及び図１９に示したものとそれぞれ等しい。また、端末認証サーバ７－８には表９に示すＶＬＡＮ情報テーブルが設けられており、ＶＬＡＮ－ＩＤの代わりにネットワークアドレスを使用している点で表３（第３実施形態）と相違している。なお、本実施形態においても、第３実施形態と同様に、無線パケット網が各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１１６】

【表９】

VLAN情報テーブル

ネットワークアドレス	VLAN鍵
ネットワークアドレス #A	VLAN鍵#a
ネットワークアドレス #B	VLAN鍵#b

【０１１７】図２２は本実施形態におけるパケット転送手順を示しており、図９に示した第３実施形態の手順とは以下の点が相違する。まず、受信したデータパケット（８－１）の改竄が検出されなかった場合、第９実施形態と同様にして、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信したデータパケットの宛先アドレス４－１から抽出されるネットワークアドレスが、無線パケット端末７－７に対して通信が許可されている複数のユーザＬＡＮ１－４に割り当てたネットワークアドレスの中に登録されているかどうかを確認する（２６－１）。そしてフィルタリング手段１６はこの確認結果に応じてパケットを転送する（８－２）か廃棄するかを決定する。

【０１１８】ここで、データパケットを転送する際（８－２）に、宛先端末がユーザＬＡＮ７－４と接続している場合、各中継ノード７－９はデータパケット中の宛先アドレス４－１に応じて次の送信ポートを選択してゲートウェイ７－３へデータパケットを転送する。ゲートウェイ７－３は宛先アドレス４－１から抽出されるネットワークアドレスに応じてゲートウェイ７－１又はゲートウェイ７－２を選択して、データパケットをユーザＬＡＮ７－４から宛先端末に転送する。一方、宛先端末が無線パケット網と接続している場合は、第３実施形態と同様に、各中継ノード７－９は宛先アドレス４－１に応じて次の送信ポートを選択して、ゲートウェイを介することなくパケットを宛先端末へ転送する。

【０１１９】本実施形態におけるブロードキャストパケットの転送手順は基本的に第３実施形態（図１０）と同様であって、ＶＬＡＮ－ＩＤの代わりに宛先アドレスから抽出されるネットワークアドレスを用いて経路選択が行われる点が相違している。

【０１２０】以上のように、本実施形態においても、第１実施形態のようにデータパケット中にＶＬＡＮ－ＩＤのような余分なフィールドを設ける必要がない。なお、ここではネットワークアドレスの使用を第３実施形態へ適用した場合について説明したが、第３実施形態と第４～第５実施形態とでは無線パケット端末７－７から無線基地局７－６へデータパケットを送信する際の暗号鍵の使い方が異なるだけである。したがって、これら第４～第５実施形態においてもＶＬＡＮ－ＩＤの代わりにネットワークアドレスを使用することができる。

【０１２１】【第１１実施形態】この第１１実施形態は、請求項１、６記載のパケット転送方法を適用した場合に相当している。

【０１２２】本実施形態におけるパケット網の構成、無線基地局の構成、無線パケット端末の認証手順及びデータパケットの改竄検出手順は、図１～図４に示した第１実施形態の場合とそれぞれ等しい。

【０１２３】表１０は、本実施形態における端末情報テーブルを示しており、端末アドレスと、端末認証に必要な情報としての暗号鍵とで構成されている。

【０１２４】

【表１０】

第１２実施形態における端末情報テーブル

端末ｱﾄﾞﾚｽ	暗号鍵
ｱﾄﾞﾚｽ#1	暗号鍵#a
ｱﾄﾞﾚｽ#2	暗号鍵#b
ｱﾄﾞﾚｽ#3	暗号鍵#c

【０１２５】各ユーザＬＡＮ１－４に接続するゲートウェイ１－１，１－２は、それぞれ許可アドレス情報を許可アドレステーブルに持っている。表１１はゲートウェイ１－１の許可アドレステーブルを示しており、表１２はゲートウェイ１－２の許可アドレステーブルを示している。ゲートウェイ１－１、１－２は、送信元アドレス４－２が各ゲートウェイの許可アドレステーブルに登録

されているデータパケットだけをユーザＬＡＮ１－４に転送する。

【０１２６】

【表１１】

ゲートウェイ1-1,7-1の許可アドレステーブル

許可ｱﾄﾞﾚｽ
ｱﾄﾞﾚｽ#1
ｱﾄﾞﾚｽ#2
－

【０１２７】

【表１２】

ゲートウェイ1-2,7-2の許可アドレステーブル

許可ｱﾄﾞﾚｽ
ｱﾄﾞﾚｽ#3
--
－

【０１２８】また、本実施形態における無線パケット網のパケットの信号フォーマットは、第８実施形態で説明した図１９のものと同じであって、宛先アドレス４－１と送信元アドレス４－２をヘッダ情報として持っており、ユーザデータ４－４は暗号化される。

【０１２９】図２３は、本実施形態におけるパケット転送手順を示している。無線基地局１－６では、端末認証手段１０が通信開始時に無線パケット端末１－７に対する認証を行い、当該パケット端末が正規の端末の場合は暗号通信を開始する。なお、この認証に際して端末認証手段１０は端末認証サーバ１－８から端末情報を得る。次に、無線パケット端末１－７は暗号化されたデータパケットを無線基地局１－６に送信する（１４－１）。無線基地局１－６ではパケット復号化手段１３がデータパケットを復号化して、パケット改竄検出手段１４が受信データパケット（１４－１）の改竄を検出した場合はこの受信データパケットを廃棄する。なお、これまでの手順は第１実施形態（図６）と同じである。一方、改竄が検出されない場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は第１実施形態のようにＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することはせず、受信データパケットをそのままフィルタリング手段１６に送出し、フィルタリング手段１６は宛先アドレス４－１で指定された宛先端末にデータパケットを転送する（１４－２）。この時、宛先端末がユーザＬＡＮ１－４と接続していれば、データパケットはゲートウェイ１－３からゲートウェイ１－１又はゲートウェイ１－２を介してユーザＬＡＮ１－４に転送される。その際、選択されたゲートウェイはデータパケット中の送信元アドレス４－２を確認し、当該アドレスが選択されたゲートウェイの許可

アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ１－４に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末に転送される。

【０１３０】以上のように、本実施形態では、通信開始時に端末認証することによって、無線パケット端末を特定可能であり、未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止することができる。また、暗号化してパケットを転送することにより、不正な端末が認証された正規の端末になりすますことを防止可能であり、なりすまし端末による不正アクセスを防止することができる。さらに、暗号の復号時に改竄を検出してパケットを廃棄することにより、改竄されたパケットの転送を防止可能であり、改竄データによる通信の妨害と無線パケット網のトラヒック増加を防止することができる。加えて、ゲートウェイが宛先アドレスと送信元アドレスに応じてパケットの転送を許可することで、認証されたパケット端末が通信の許可されていないユーザＬＡＮにアクセスするのを防止可能であり、他ユーザＬＡＮに所属している端末からの不正アクセスを防止することができる。

【０１３１】〔第１２実施形態〕この第１２実施形態は、請求項１，７，８記載のパケット転送方法を適用した場合に相当している。

【０１３２】本実施形態におけるパケット網の構成は図８に示す第３実施形態の構成に等しい。また、本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【０１３３】第３実施形態と同様に、ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【０１３４】端末認証サーバ７－８は第３実施形態と同様に端末情報テーブルとＶＬＡＮ情報テーブルを有している。本実施形態におけるＶＬＡＮ情報テーブルは、表３に示す第３実施形態におけるＶＬＡＮ情報テーブルに等しい。本実施形態では、ＶＬＡＮ鍵がブロードキャストパケット及びマルチキャストパケットの暗号化に使用される。なお、無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１３５】本実施形態における端末情報テーブルは、表１０に示す第１１実施形態における情報テーブルと等しい。この端末情報テーブルに登録した暗号鍵（端末鍵）は、端末認証及びユニキャストパケットの暗号化に用いられる。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【０１３６】各ユーザＬＡＮ７－４に接続するゲートウェイ７－１，７－２は、第１１実施形態におけるゲート

ウェイ１－１，１－２と同様に、許可アドレス情報を表１１，表１２に示した許可アドレステーブルに持っている。

【０１３７】図２４は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、無線パケット端末７－７は第３実施形態と同様にパケットに応じた暗号鍵としてＶＬＡＮ鍵又は端末鍵を選択し、暗号化されたデータパケットを無線基地局７－６に送信する（１５－１）。無線基地局７－６は第３実施形態と同様にパケットに応じた復号鍵を選択してデータパケットを復号化する。そして、パケット改竄検出手段１４が受信データパケット（１５－１）の改竄を検出した場合はこの受信データパケットを廃棄する。一方、改竄が検出されない場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は第３実施形態のようにＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することはせず、受信データパケットをそのままフィルタリング手段１６に送出し、フィルタリング手段１６は宛先アドレス４－１で指定される宛先端末に転送するためにデータパケットを無線パケット網へ送信する（１５－２）。この時、宛先端末がユーザＬＡＮ７－４と接続している場合、各中継ノード７－９はデータパケット中の宛先アドレス４－１に応じて次の送信ポートを選択してゲートウェイ７－３へデータパケットを転送する。ゲートウェイ７－３は宛先アドレス４－１から抽出されるネットワークアドレスに応じてゲートウェイ７－１又はゲートウェイ７－２を選択し、選択されたゲートウェイに接続するユーザＬＡＮ７－４から宛先端末にデータパケットを転送する（１５－３）。その際、選択されたゲートウェイはデータパケット中の送信元アドレス４－２を確認し、当該アドレスが選択されたゲートウェイの許可アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ７－４に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合は、第３実施形態と同様に、各中継ノード７－９は宛先アドレス４－１に応じて次の送信ポートを選択して、ゲートウェイを介することなくデータパケットを宛先端末へ転送する。

【０１３８】本実施形態におけるブロードキャストパケットの転送手順は、図１０に示す第３実施形態の場合と等しい。本実施形態では、暗号化にＶＬＡＮ鍵を用いているため、第３実施形態と同様に、ＶＬＡＮ－ＩＤの同じパケット端末は、ブロードキャストパケット及びマルチキャストパケットの復号が可能である。

【０１３９】また、本実施形態においてブロードキャストパケットをパケット網が転送する様子は、図１１に示す第３実施形態の場合と等しい。

【０１４０】以上のように、本実施形態によれば、第１１実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、ＶＬＡＮ－ＩＤにより次の中継ノードを選択してパケットを転送するため、同じＶＬＡＮ－ＩＤを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり、最適な経路選択で転送することが可能であって、転送遅延時間，トラヒック，ゲートウェイの処理負荷の増加を防止することができる。また、ブロードキャストパケット又はマルチキャストパケットを転送する際は、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため、無線基地局は同じＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して１回の送信でこれらパケットを転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制することができる。なお、ＶＬＡＮ鍵は端末固有の暗号鍵ではないが、異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【０１４１】〔第１３実施形態〕この第１３実施形態は、請求項１，７，９記載のパケット転送方法を適用した場合に相当している。

【０１４２】本実施形態におけるパケット網の構成は図８に示す第３実施形態の構成に等しい。また、本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【０１４３】第３実施形態と同様に、ＶＬＡＮ－ＩＤは各ユーザＬＡＮに固有の値があらかじめ割り当てられている。端末認証サーバ７－８は第３実施形態と同様に端末情報テーブルとＶＬＡＮ情報テーブルを有している。本実施形態におけるＶＬＡＮ情報テーブルは、表３に示す第３実施形態におけるＶＬＡＮ情報テーブルに等しい。

【０１４４】本実施形態において、ＶＬＡＮ鍵は無線基地局７－６がブロードキャストパケット及びマルチキャストパケットを暗号化するときに使用される。なお、無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１４５】また、本実施形態における端末情報テーブ

ルは表１０に示す第１１実施形態の端末情報テーブルと等しい。この端末情報テーブルに登録した暗号鍵（端末鍵）は、端末認証時，ユニキャストパケットの暗号化時、ならびに、無線パケット端末７－７によるブロードキャスト及びマルチキャストパケットの暗号化時においてそれぞれ用いられる。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【０１４６】ゲートウェイ７－１，７－２は第１１実施形態におけるゲートウェイ１－１，１－２と同様に、表１１，表１２に示す許可アドレステーブルをそれぞれ有している。

【０１４７】図２５は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い，当該パケット端末が正規の端末であれば暗号通信を開始する。なお，この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、無線パケット端末７－７は第４実施形態と同様にユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく端末鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１６－１）。無線基地局７－６では、パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなく端末鍵を用いてデータパケットを復号化する。これ以後は，第１２実施形態と同様に、無線基地局７－６は受信したデータパケットが改竄されていればパケットを廃棄し，改竄されていない場合は、ＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することなく、第１２実施形態と同様にして宛先アドレス４－１で指定される宛先端末までデータパケットを転送する（１６－３），すなわち，宛先端末がユーザＬＡＮ７－４と接続しているならば，データパケットは各中継ノード７－９，ゲートウェイ７－３，ゲートウェイ７－１又はゲートウェイ７－２，ユーザＬＡＮ７－４を経て宛先端末に転送される。その際、ゲートウェイ７－１又は７－２はデータパケット（１６－２）の送信元アドレス４－２が許可アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ７－４に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合，データパケットはゲートウェイを介することなく宛先端末へ転送される。

【０１４８】また、本実施形態においてブロードキャストパケットをパケット網が転送する様子は図１１に示す第３実施形態の場合に等しい。

【０１４９】本実施形態によれば、第１１実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は，ＶＬＡＮ－ＩＤにより次の中継ノードを選択してパケットを転送するため，同じＶＬＡＮ－ＩＤを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり，最適な経路選択で転送することが可能であって、転送遅延時間，トラヒック，ゲートウェイの処理負荷の増加を防止することができる。また，無線基地局が送信するブロードキャストパケット及びマルチキャストパケットの暗号化の際にはＶＬＡＮ鍵を用いるため，ＶＬＡＮ－ＩＤの同じパケット端末は暗号の復号が可能である。また、無線基地局がブロードキャストパケット又はマルチキャストパケットを転送する際は、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため，無線基地局は同じＶＬＡＮ－ＩＤを待つ配下の全無線パケット端末に対して１回の送信でこれらパケットを転送することができる。したがって，各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて，トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制することができる。さらに，無線パケット端末は，送信するブロードキャストパケット及びマルチキャストパケットの暗号化に際して、ユニキャストパケット用の暗号鍵である端末鍵を用いている。そのため、第１２実施形態などとは異なり、無線基地局はパケットの受信時に２種類の暗号鍵を切り替えることなく暗号を復号することが可能となる。したがって，ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて，無線基地局の負荷を抑制することができる。

【０１５０】【第１４実施形態】この第１４実施形態は，請求項１，７，１０記載のパケット転送方法を適用した場合に相当している。

【０１５１】本実施形態におけるパケット網の構成は図８に示す第３実施形態の構成に等しい。また、本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【０１５２】第３実施形態と同様に，ＶＬＡＮ－ＩＤは各ユーザＬＡＮに対して固有の値があらかじめ割り当てられている。端末認証サーバ７－８は第３実施形態と同様に端末情報テーブルとＶＬＡＮ情報テーブルを有している。本実施形態におけるＶＬＡＮ情報テーブルは、表３に示す第３実施形態におけるＶＬＡＮ情報テーブルに等しい。本実施形態では，第５実施形態と同様に，ＶＬＡＮ鍵はパケットを暗号化するときに使用される。な

お．無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１５３】本実施形態における端末情報テーブルは表１０に示した第１１実施形態の端末情報テーブルと等しい。また、端末情報テーブルに登録した暗号鍵としては．各端末が所属するユーザＬＡＮ７－４のＶＬＡＮ鍵を用いる。

【０１５４】ゲートウェイ７－１，７－２は第１１実施形態におけるゲートウェイ１－１，１－２と同様に、それぞれ表１１、表１２に示す許可アドレステーブルを有している。

【０１５５】図２６は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い．当該パケット端末が正規の端末であれば暗号通信を開始する。なお．この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、無線パケット端末７－７は第５実施形態と同様にユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なくＶＬＡＮ鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１７－１）。無線基地局７－６では．パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなくＶＬＡＮ鍵を用いてデータパケットを復号化する。これ以後は．第１２実施形態と同様に、無線基地局７－６は受信したデータパケットが改竄されていればパケットを廃棄し．改竄されていない場合は、ＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することなく．第１２実施形態と同様にして宛先アドレス４－１で指定される宛先端末までデータパケットを転送する（１７－３）。すなわち．宛先端末がユーザＬＡＮ７－４と接続しているならば．データパケットは各中継ノード７－９，ゲートウェイ７－３，ゲートウェイ７－１又はゲートウェイ７－２，ユーザＬＡＮ７－４を経て宛先端末に転送される。その際．ゲートウェイ７－１又は７－２はデータパケット（１７－２）の送信元アドレス４－２が許可アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ７－４に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末へ転送される。

【０１５６】本実施形態においてブロードキャストパケットをパケット網が転送する様子は．図１１に示す第３実施形態の場合と等しい。

【０１５７】以上のように．本実施形態によれば．第１１実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち．宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には．ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって．転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、ＶＬＡＮ－ＩＤにより次の中継ノードを選択してパケットを転送するため、同じＶＬＡＮ－ＩＤを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり、最適な経路選択で転送することが可能であって．転送遅延時間，トラヒック．ゲートウェイの処理負荷の増加を防止することができる。また、本実施形態では、暗号化にＶＬＡＮ鍵のみを用いるようにして端末鍵を用いないため、ＶＬＡＮ－ＩＤの同じパケット端末はブロードキャスト及びマルチキャストパケットの暗号を復号することが可能である。また．ＶＬＡＮ－ＩＤに共通する暗号鍵を用いているため．無線基地局及び無線パケット端末はパケット受信時に２種類の暗号鍵を切り替えて暗号化及び復号する必要がない。したがって、２種類の暗号鍵を用いる場合に比べて．無線基地局及び無線パケット端末の負荷を抑制することができる。また、パケットを転送する際は．ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため．無線基地局は同じＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して１回の送信でこれらパケットを転送することができる。したがって．各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて．トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制することができる。なお、ＶＬＡＮ鍵は端末固有の暗号鍵ではないが、異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【０１５８】【第１５実施形態】上述した各実施形態では本発明を無線パケット網へ適用した場合について説明してきたが、本発明は無線パケット網に限らず有線パケット網に適用しても良い。図２７は．前述した第１実施形態を有線パケット網で実現した場合のネットワーク構成を示している。同図では．無線パケットバックボーン網１－５と同等の機能を有するパケットバックボーン網２７－５，無線／有線の違いを除いて無線基地局１－６と同等の機能を有するアクセスサーバ（有線接続装置）２７－６，および無線／有線の違いを除いて無線パケット端末１－７と同等の機能を有するパケット端末２７－７がそれぞれ設けられている。これら以外の構成は全て第１実施形態（図１）と同じである。本実施形態によるパケット転送手順は、アクセスサーバ２７－６とパケット端末２７－７の間を含めた全ての通信が有線で行われる点を除けば．第１実施形態と全く同じになる。また、図８に示したネットワーク構成を用いる場合にも．無線パケットバックボーン網７－５，無線基地局７－６，無線パケット端末７－７をそれぞれパケットバックボーン

網２７－５，アクセスサーバ２７－６，パケット端末２７－７に置き換えれば良い。したがって、上述した全ての実施形態に対して有線パケット網のネットワーク構成を適用することができる。

【０１５９】以上述べた実施形態は全て本発明を例示的に示すものであって限定的に示すものではなく，本発明は他の種々の変形態様及び変更態様で実施することができる。従って本発明の範囲は特許請求の範囲及びその均等範囲によってのみ規定されるものである。

【０１６０】例えば、上記各実施形態では、パケット網への入口である無線基地局（あるいはアクセスサーバ）が端末認証やパケット改竄検出などを行うことによって，最も効率的な転送を実現することができる。しかしながら、パケット網の構成によっては無線基地局を統括する制御局などが設けられている場合もあり、そうした場合には、この制御局が端末認証やパケット改竄検出を行うようにしても良い。

【０１６１】

【発明の効果】以上説明したように，本発明によれば、通信開始時に端末認証することによってパケット端末を特定可能であり，未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止する効果が得られる。また，暗号化してパケットを転送することにより，不正な端末が認証された正規の端末になりすますことを防止可能であり、なりすまし端末による不正アクセスを防止する効果が得られる。さらに，暗号の復号時に改竄を検出してパケットを廃棄することにより，改竄されたパケットの転送を防止可能であり，改竄データによる通信の妨害とパケット網のトラヒック増加を防止する効果が得られる。

【０１６２】従って、送信元アドレスを偽造することによりデータ網（ユーザＬＡＮ）へ不正にアクセスできる問題を解決し，あらかじめ登録した端末に対してだけ特定のデータ網との通信を許可するパケット転送方法を提供することが可能となる。また、パケットの転送遅延時間，トラヒック，ゲートウェイの負荷が増加する問題を解決し、最適な経路選択が可能でなおかつ効率的なパケット転送方法を提供することが可能となる。

【０１６３】また、請求項２，３，１１又は１２記載の発明によれば，識別子又はユーザＬＡＮ名と送信元アドレスの対応を確認することにより，認証された端末が自分が接続の許可されていない（あるいは自分の属していない）データ網にアクセスすることを防止可能であり、あるデータ網に接続を許可されている（あるいは所属している）端末から他データ網への不正アクセスを防止する効果が得られる。さらにまた，１パケット端末あたり複数の識別子又はユーザＬＡＮ名を登録することにより，１つのパケット端末で複数のデータ網にアクセスすることが可能であり、ユーザへのサービス性が向上するという効果が得られる。

【０１６４】また、請求項４又は７記載の発明によれば，宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、パケット端末が他のパケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であり，転送遅延時間の増加を防止する効果が得られる。また，ブロードキャストパケット及びマルチキャストパケットを転送する場合は、識別子に応じて次の中継ノードを選択してパケットを転送するため，同じ識別子を用いて通信している全てのパケット端末に対してゲートウェイからユニキャスト転送する必要がない。したがって、最適な経路選択でパケットを転送することが可能であり，転送遅延時間，トラヒック，ゲートウェイの処理負荷の増加をそれぞれ防止する効果が得られる。

【０１６５】また、請求項６記載の発明によれば，ゲートウェイが宛先アドレスと送信元アドレスに応じてパケットの転送を許可することで、認証されたパケット端末が通信の許可されていないユーザＬＡＮにアクセスすることを防止可能であり、他ユーザＬＡＮに所属しているパケット端末からの不正アクセスを防止する効果が得られる。

【０１６６】また、請求項８又は１３記載の発明によれば，識別子が同じであれば共通の暗号鍵を用いてブロードキャストパケット及びマルチキャストパケットを暗号化しているため，基地局は同一の識別子を持つ配下の全パケット端末に対して１回の送信でこれらパケットを転送することが可能となる。したがって，各パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて，トラヒック，転送遅延時間，基地局の負荷を抑制する効果が得られる。

【０１６７】また、請求項９又は１４記載の発明によれば，基地局がブロードキャストパケット及びマルチキャストパケットを転送する際には、識別子に共通する暗号鍵を用いて暗号化している。このため，基地局は同じ識別子を持つ配下の全パケット端末に対して１回の送信でこれらパケットを転送することが可能となる。したがって，各パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて，トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制する効果が得られる。また、パケット端末がブロードキャストパケット及びマルチキャストパケットを転送する際には、ユニキャストパケット用の暗号鍵を用いて暗号化している。したがって、基地局はパケット端末からパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となり，ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて，基地局にかかる負荷を抑制する効果が得られる。

【０１６８】また、請求項１０又は１５記載の発明によれば，パケットを転送する際、識別子に共通の暗号鍵を用いて暗号化しているため，基地局は同じ識別子を有す

る配下の全パケット端末に対して１回の送信でブロードキャストパケット及びマルチキャストパケットを転送することが可能となる。したがって、各パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制する効果が得られる。また、識別子に共通する暗号鍵を用いているため、基地局及びパケット端末はパケットの受信時において暗号鍵を切り替えることなく復号することが可能となる。したがって、２種類の暗号鍵を用いる場合に比べて，基地局及びパケット端末にかかる負荷を抑制する効果が得られる。

【図面の簡単な説明】

【図１】　本発明の第１実施形態における無線パケット通信のネットワーク構成を示すブロック図である。

【図２】　本発明の各実施形態における無線基地局の構成を示すブロック図である。

【図３】　本発明の第１実施形態における無線パケット通信の認証手順を示す図である。

【図４】　同実施形態におけるデータパケットの改竄検出手順を示す図である。

【図５】　同実施形態におけるパケットの信号フォーマットを示す図である。

【図６】　同実施形態におけるパケット転送手順を示す図である。

【図７】　本発明の第２実施形態におけるパケット転送手順を示す図である。

【図８】　本発明の第３実施形態における無線パケット通信のネットワーク構成を示すブロック図である。

【図９】　同実施形態におけるパケット転送手順を示す図である。

【図１０】　同実施形態におけるブロードキャストパケットの転送手順を示す図である。

【図１１】　同実施形態におけるブロードキャストパケットの転送の様子を示す図である。

【図１２】　本発明の第４実施形態におけるパケット転送手順を示す図である。

【図１３】　本発明の第５実施形態におけるパケット転送手順を示す図である。

【図１４】　本発明の第６実施形態における無線パケット通信の認証手順を示す図である。

【図１５】　同実施形態におけるパケット転送手順を示す図である。

【図１６】　本発明の第７実施形態における無線パケット通信の認証手順を示す図である。

【図１７】　同実施形態におけるパケット転送手順を示す図である。

【図１８】　ＩＰアドレスの構成を示す図である。

【図１９】　本発明の第８実施形態におけるパケットの信号フォーマットを示す図である。

【図２０】　同実施形態におけるパケット転送手順を示す図である。

【図２１】　本発明の第９実施形態におけるパケット転送手順を示す図である。

【図２２】　本発明の第１０実施形態におけるパケット転送手順を示す図である。

【図２３】　本発明の第１１実施形態におけるパケット転送手順を示す図である。

【図２４】　本発明の第１２実施形態におけるパケット転送手順を示す図である。

【図２５】　本発明の第１３実施形態におけるパケット転送手順を示す図である。

【図２６】　本発明の第１４実施形態におけるパケット転送手順を示す図である。

【図２７】　本発明の第１５実施形態における有線パケット通信のネットワーク構成を示すブロック図である。

【符号の説明】

１－１、１－２．１－３．７－１、７－２、７－３　ゲートウェイ

１－４、７－４　ユーザＬＡＮ

１－５、７－５　無線パケットバックボーン網

１－６、７－６．７－６ａ～７－６ｃ　無線基地局

１－７、７－７．７－７ａ～７－７ｃ　無線パケット端末

１－８、７－８　端末認証サーバ

１－１０、７－１０　中継路

４－１　宛先アドレス

４－２　送信元アドレス

４－３　ＶＬＡＮ－ＩＤ

４－４　ユーザデータ

７－９、７－９ａ～７－９ｃ　中継ノード

１０　端末認証手段

１１　端末情報記憶手段

１２　パケット暗号化手段

１３　パケット復号化手段

１４　パケット改竄検出手段

１５　端末アドレス／ＶＬＡＮ－ＩＤ比較手段

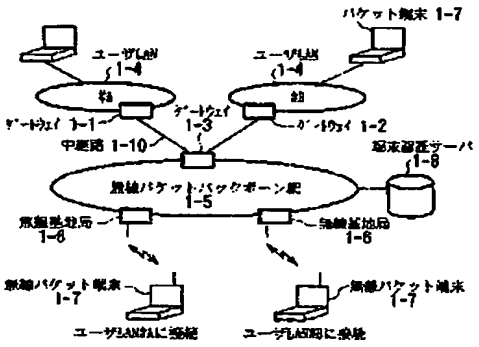
１６　フィルタリング手段

２７－５　パケットバックボーン網

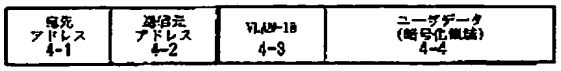
２７－６　アクセスサーバ（有線接続装置）

２７－７　パケット端末

【図１】

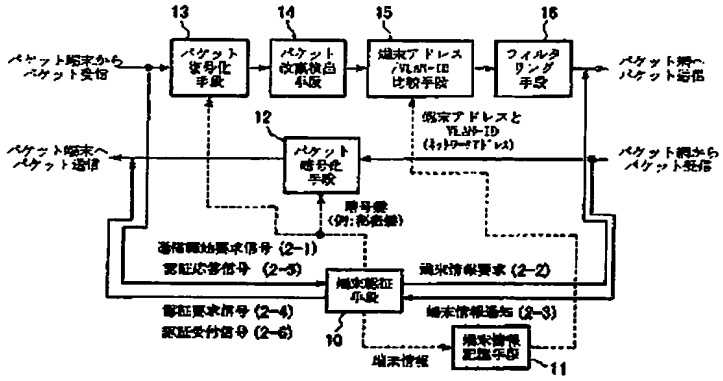


【図５】

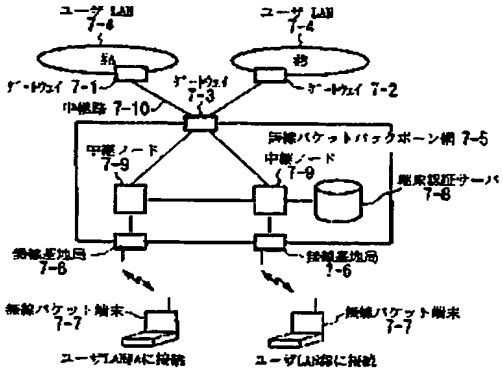


【図１８】

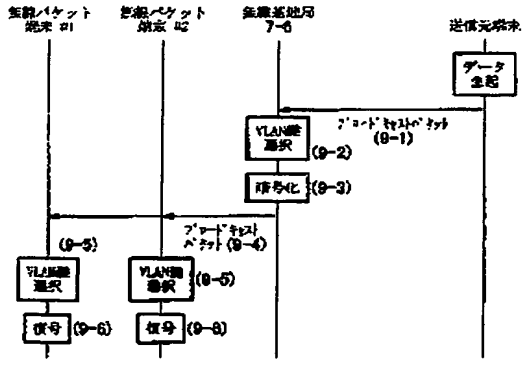
【図２】



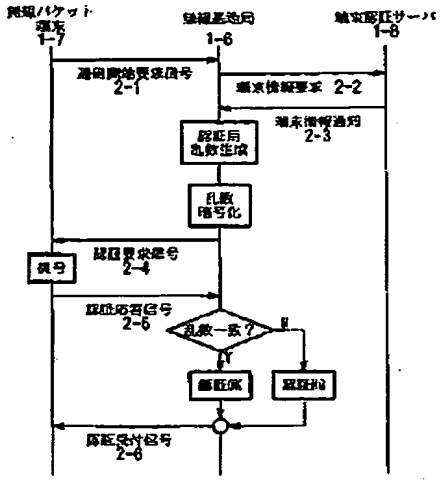
【図８】



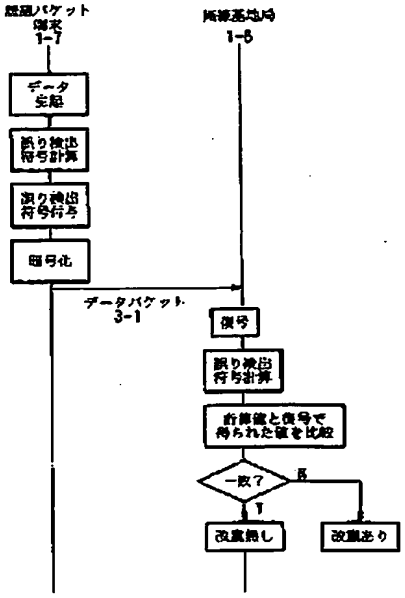
【図１０】



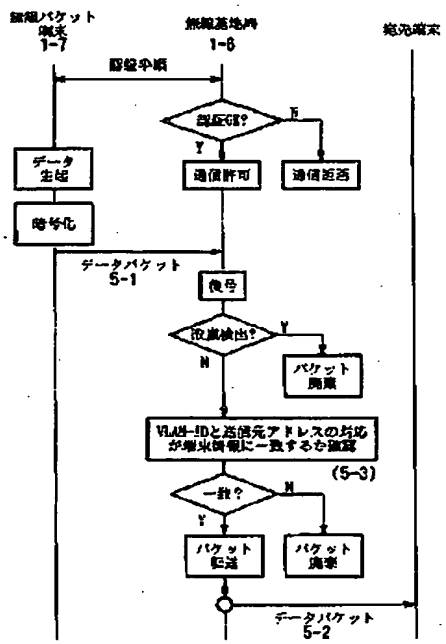
【図３】


無線パケット端末 1-7
無線基地局 1-6
端末認証サーバ 1-8
通信開始要求信号 2-1
端末情報要求 2-2
端末情報通知 2-3
認証用乱数生成
乱数暗号化
復号
認証要求信号 2-4
認証応答信号 2-5
乱数一致?
Y
N
認証OK
認証NG
認証受付信号 2-6

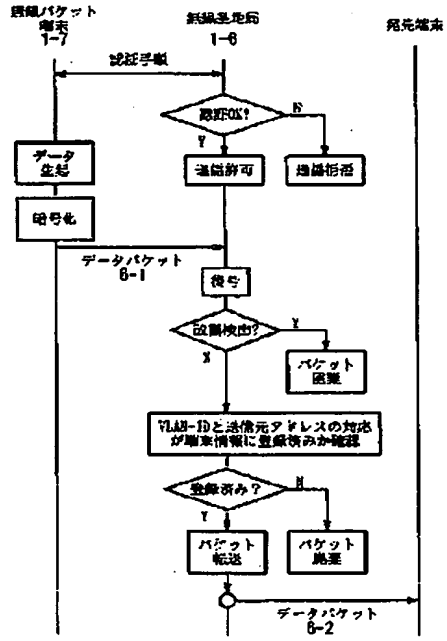
【図４】


無線パケット端末 1-7
無線基地局 1-6
データ生起
誤り検出符号計算
誤り検出符号付与
暗号化
データパケット 3-1
復号
誤り検出符号計算
計算値と復号で得られた値を比較
一致?
Y
N
改竄なし
改竄あり

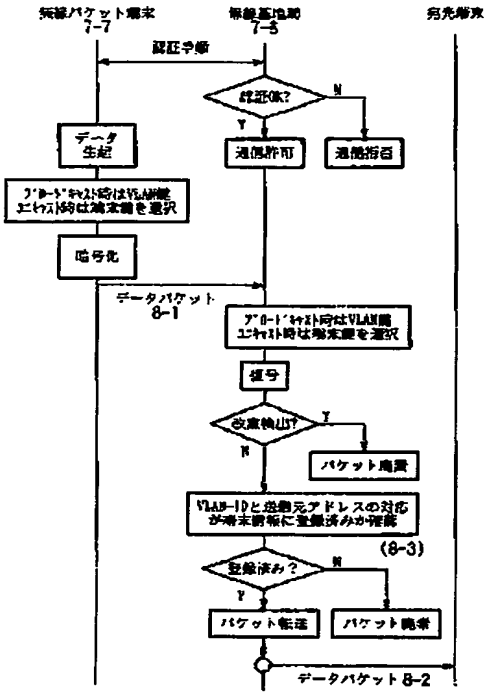
【図６】


無線パケット端末 1-7
無線基地局 1-6
宛先端末
認証手順
認証OK?
Y
N
データ生起
通信許可
通信拒否
暗号化
データパケット 5-1
復号
改竄検出?
Y
N
パケット廃棄
VLAN-IDと送信元アドレスの対応が端末情報に一致するか確認 (5-3)
一致?
Y
N
パケット転送
パケット廃棄
データパケット 5-2

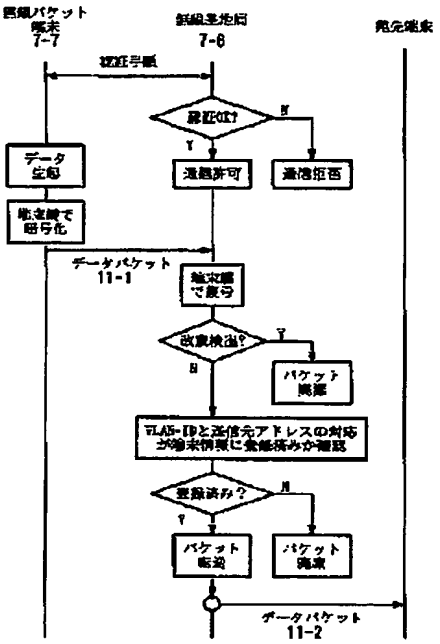
【図７】


無線パケット端末 1-7
無線基地局 1-6
宛先端末
認証手順
認証OK?
Y
N
データ生起
通信許可
通信拒否
暗号化
データパケット 6-1
復号
改竄検出?
Y
N
パケット廃棄
VLAN-IDと送信元アドレスの対応が端末情報に登録済みか確認
登録済み?
Y
N
パケット転送
パケット廃棄
データパケット 6-2

【図９】

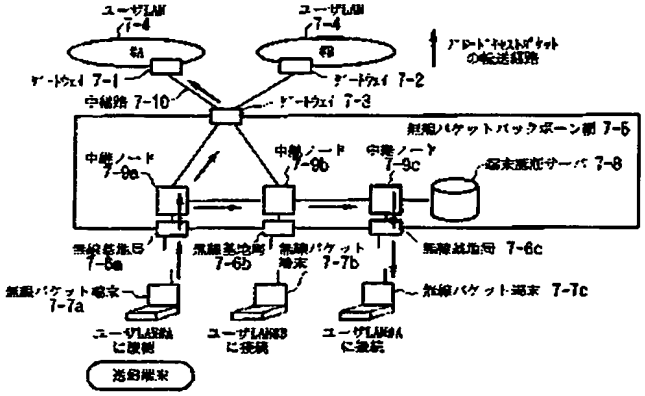


【図１２】

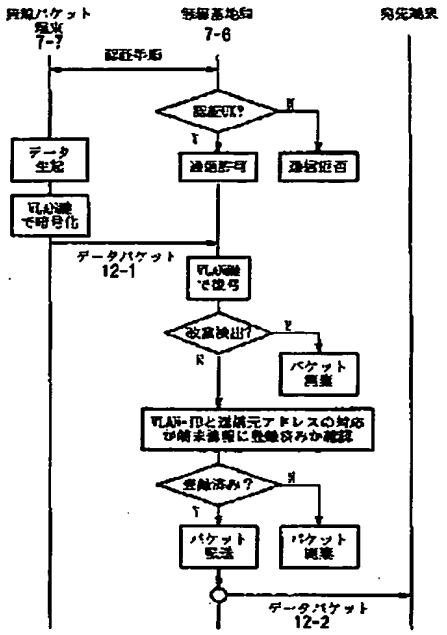


【図１９】

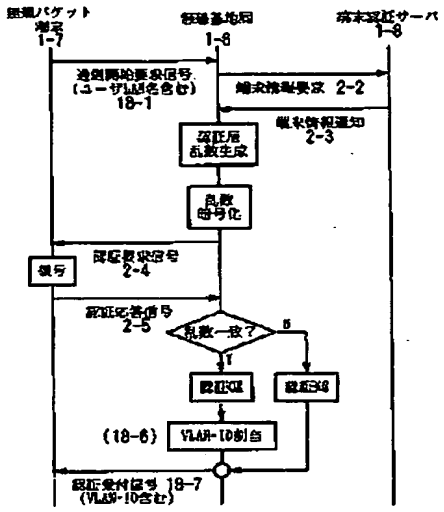
【図１１】



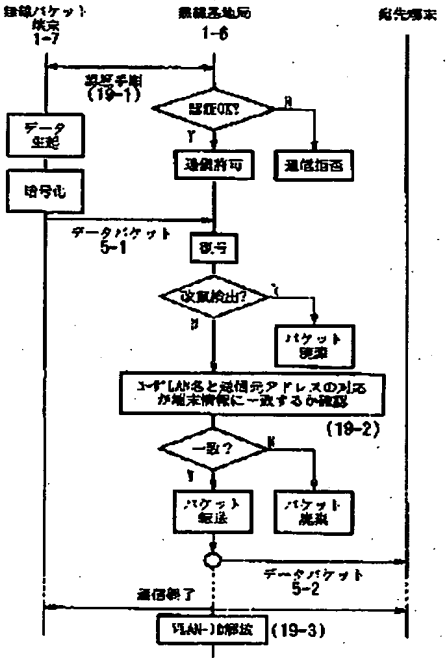
【図１３】



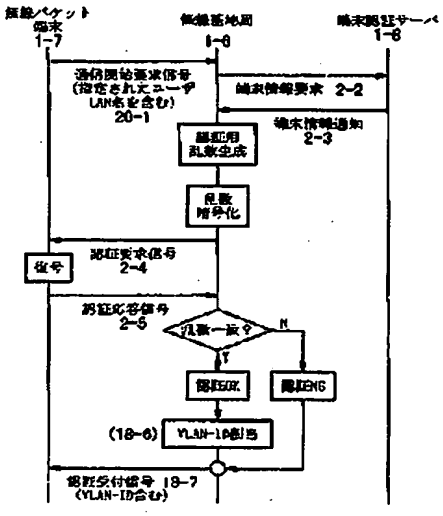
【図１４】



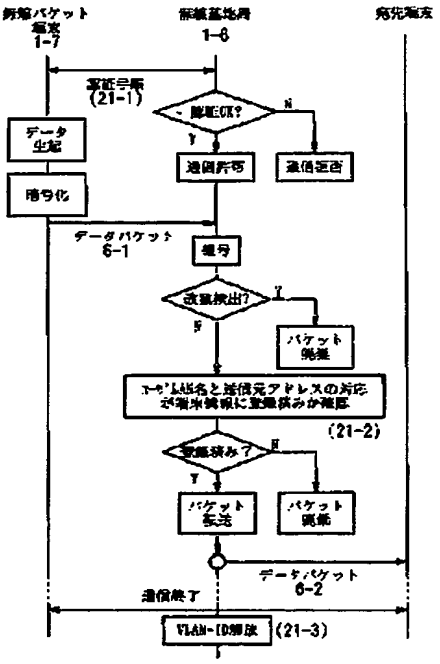
【図１５】



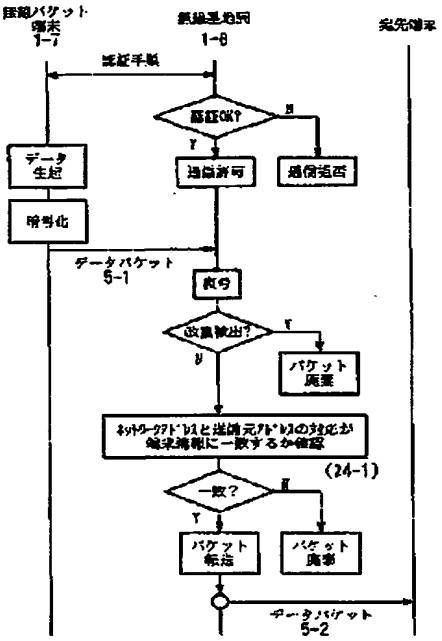
【図１６】



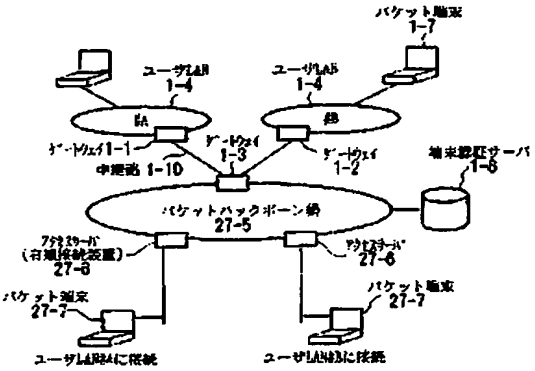
【図１７】


データ生起
暗号化
データパケット 6-1
暗号
パケット廃棄
パケット転送
パケット廃棄
データパケット 6-2
通信終了
(21-1)
(21-2)
(21-3)

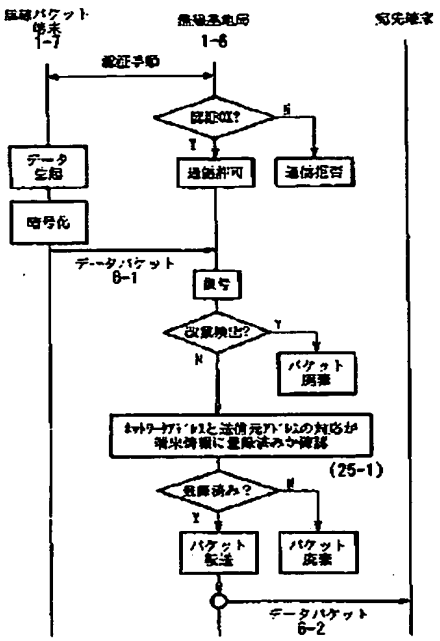
【図２０】


データ生起
暗号化
データパケット 5-1
パケット廃棄
パケット転送
パケット廃棄
データパケット 5-2
(24-1)

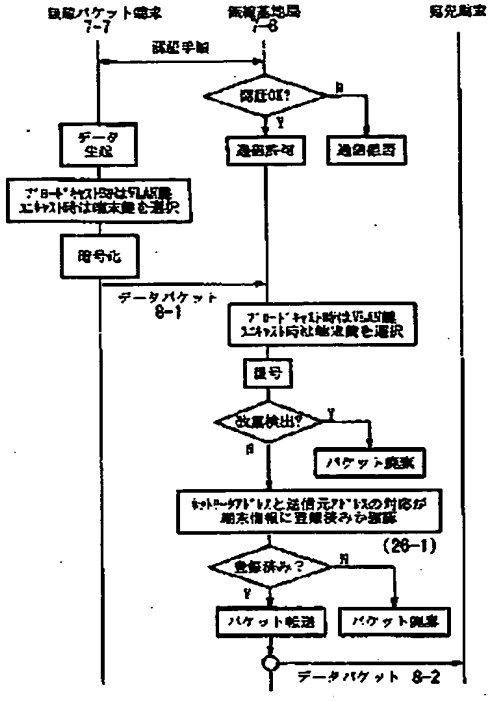
【図２７】


パケット端末 1-7
ユーザLAN 1-4
ユーザLAN 1-4
ゲートウェイ 1-1
ゲートウェイ 1-3
ゲートウェイ 1-2
端末認証サーバ 1-6
パケットバックボーン網 27-5
パケット端末 27-7
パケット端末 27-7
ユーザLAN#4に接続
ユーザLAN#3に接続

【図２１】

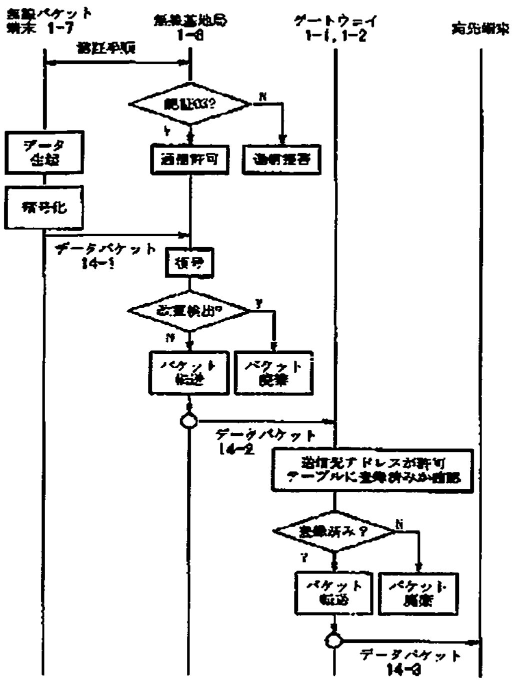

1-7
1-6
認証手順
認証OK?
N
Y
データ生成
通信許可
通信拒否
暗号化
データパケット
6-1
復号
改竄検出?
Y
N
パケット廃棄
(25-1)
登録済み?
N
Y
パケット転送
パケット廃棄
データパケット
6-2

【図２２】

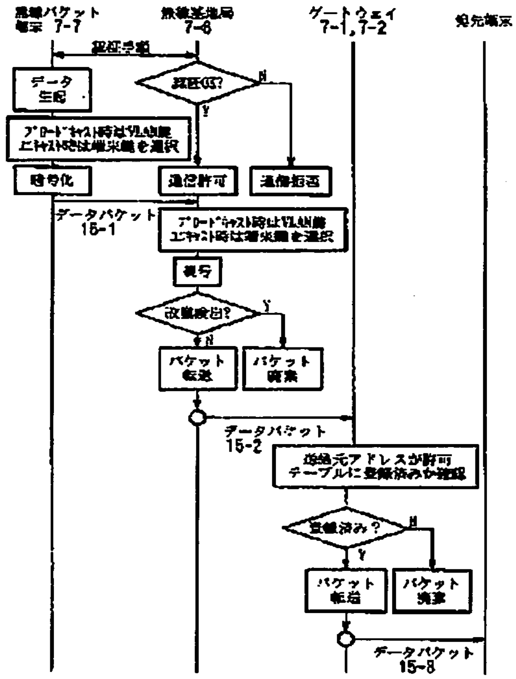

7-7
1-8
認証手順
認証OK?
N
Y
データ生成
通信許可
通信拒否
暗号化
データパケット
8-1
復号
改竄検出?
Y
N
パケット廃棄
(26-1)
登録済み?
N
Y
パケット転送
パケット廃棄
データパケット 8-2

Page 1 of 1

【図２３】

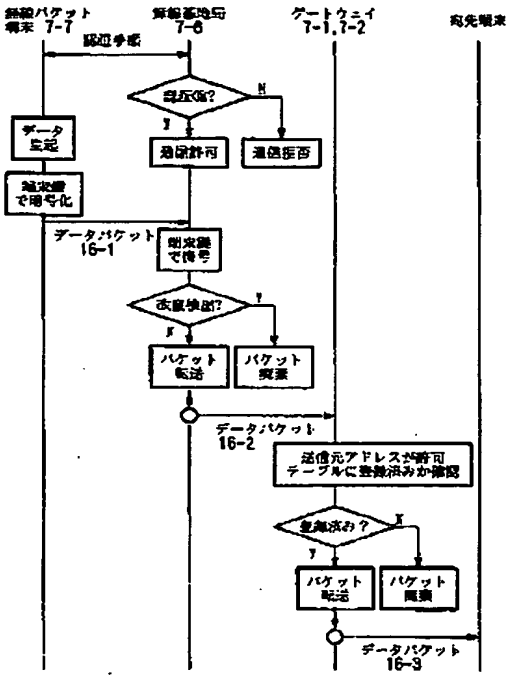


【図２４】

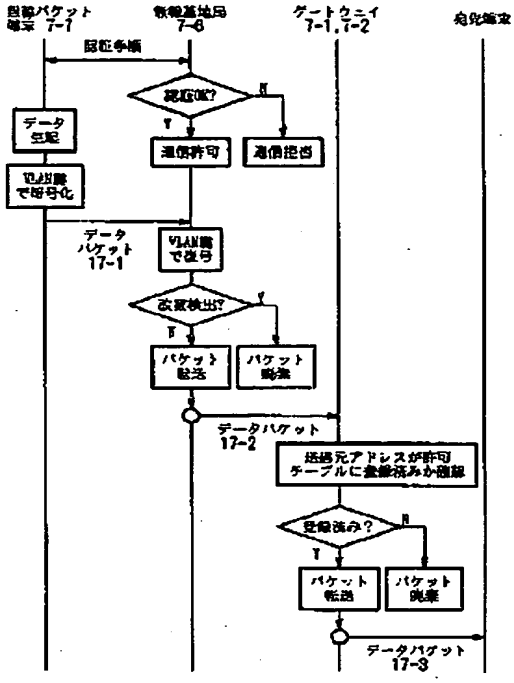


http://www4.ipdl.ncipi.go.jp/tjcontentbsen.ipdl?N0000=21&N0400=image/gif&N0401=...　3/7/2005

【図２５】



【図２６】



フロントページの続き

(72)発明者　高梨　斉
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　守倉　正博
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

する。

【００３８】以上のように，本実施形態によれば，通信開始時に端末認証することによって無線パケット端末を特定可能であり，未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止することができる。また，端末固有の暗号鍵により暗号化してパケットを転送することにより，不正な端末が認証された正規の端末になりすますことを防止可能であり，なりすまし端末による不正アクセスを防止することができる。さらに，暗号の復号時に改竄を検出してパケットを廃棄することにより，改竄されたパケットの転送を防止可能であり，改竄データによる通信の妨害と無線パケット網のトラヒック増加を防止する効果が得られる。しかも，ＶＬＡＮ－ＩＤと送信元アドレスの対応を確認することにより，認証後の端末が自分の属していないユーザＬＡＮにアクセスすることを防止可能であり，他ユーザＬＡＮに所属している端末からの不正アクセスを防止することができる。

【００３９】［第２実施形態］この第２実施形態は，請求項１，２，５記載のパケット転送方法および請求項１＊

＊１記載の基地局を適用した場合に相当している。

【００４０】本実施形態において，パケット網のネットワーク構成，無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは，それぞれ図１～図５に示した第１実施形態の場合と等しい。

【００４１】第１実施形態と同様に，ＶＬＡＮ－ＩＤは各ユーザＬＡＮ１－４に固有の値があらかじめ割り当てられている。

【００４２】各無線パケット端末１－７は，接続を許可されている複数のユーザＬＡＮ１－４のＶＬＡＮ－ＩＤを端末認証サーバ１－８にあらかじめ登録している。

【００４３】表２は，本実施形態における端末情報テーブルを示している。例えば，端末アドレスとしてアドレス＃１を持つ無線パケット端末は，ＶＬＡＮ－ＩＤとしてＶＬＡＮ－ＩＤ＃Ａ又はＶＬＡＮ－ＩＤ＃Ｂを持つユーザＬＡＮ１－４に接続が許可されている。

【００４４】

【表２】

第２の実施形態における端末情報テーブル

端末アドレス	VLAN-ID	VLAN-ID	暗号鍵
アドレス#1	VLAN-ID#A	VLAN-ID#B	暗号鍵#a
アドレス#2	VLAN-ID#A	VLAN-ID#B	暗号鍵#b
アドレス#3	VLAN-ID#B	－	暗号鍵#c

【００４５】以下に詳述するように，無線基地局１－６は，無線パケット端末１－７から受信したパケットの内，当該無線パケット端末が接続を許可されているユーザＬＡＮのＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し，何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００４６】図７は，本実施形態におけるパケット転送手順を示している。無線基地局１－６では端末認証手段１０が無線パケット端末１－７に対する認証を行い，当該無線パケット端末が正規の端末であれば暗号通信を開始する。次に，無線基地局１－６ではパケット復号化手段１３が無線パケット端末１－７からのデータパケットを復号（６－１）し，パケット改竄検出手段１４は受信データパケットの改竄を調べ，改竄が検出された場合はパケットを廃棄する。なお，これまでの手順は第１実施形態と同様である。一方，改竄が検出されない場合，無線基地局１－６では，端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５が端末情報記憶手段１１に記憶してある端末情報を参照し，ＶＬＡＮ－ＩＤ４－３と送信元アドレス４－２との対応が端末情報に登録済みであるかどうか確認してその結果をフィルタリング手段１６に送出する。すなわち，端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は，端末情報テーブル中の端末アドレスが送信元アドレス４－２に一致し，かつ，当該端末アドレスに対応して登録されている複数のＶＬＡＮ－ＩＤの中にＶＬＡＮ－ＩＤ４－３と一致するものが存在していれば，上記対応が端末情報に登録済みであるものと判断する。そして，フィルタリング手段１６は送られた確認結果に基づいて，上記対応が端末情報に登録済みであれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送する（６－２）。この時，宛先端末がユーザＬＡＮ１－４と接続しているならば，データパケットはゲートウェイ１－３からゲートウェイ１－１又はゲートウェイ１－２を介してユーザＬＡＮ１－４に転送される。また，宛先端末が無線パケット網と接続している場合，データパケットはゲートウェイを介することなく宛先端末に転送される。一方，ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に未登録の場合，フィルタリング手段１６はデータパケットを廃棄する。

【００４７】以上のように，本実施形態によれば，第１実施形態から得られる効果のほかにさらに以下の効果が得られる。すなわち，ＶＬＡＮ－ＩＤと送信元アドレスの対応を確認することにより，認証後の端末が接続の許可されていないデータ網にアクセスすることを防止可能であり，接続を許可されている端末から他データ網への不正アクセスを防止することができる。また，１無線パケット端末あたり複数のＶＬＡＮ－ＩＤを登録することにより，１つの無線パケット端末で複数のデータ網にアクセスすることが可能であり，ユーザへのサービス性が向上する。

【００４８】【第３実施形態】この第３実施形態は、請求項１，２，４，５，８記載のパケット転送方法および請求項１１，１３記載の基地局を適用した場合に相当している。

【００４９】図８は、本実施形態におけるパケット網のネットワーク構成を概略的に示している。第１実施形態と同様に、無線パケット網は、複数の無線基地局７－６と、これら複数の無線基地局７－６を接続する無線パケットバックボーン網７－５とで構成されている。各無線基地局７－６はその配下に複数の無線パケット端末７－７を収容している。無線パケットバックボーン網７－５は、ゲートウェイ７－１～７－３を介して、複数のユーザＬＡＮ７－４（他パケット網）に接続されている。ここで、ゲートウェイ７－３はＶＬＡＮ－ＩＤ４－３に応じて何れかのユーザＬＡＮ７－４を選択し、パケットからＶＬＡＮ－ＩＤを削除したのち、選択したユーザＬＡＮへパケットを転送する。さらに、本実施形態における無線パケットバックボーン網７－５はパケットを中継する複数の中継ノード７－９を有している。各中継ノード７－９は、パケット中の宛先アドレス４－１及びＶＬＡＮ－ＩＤ４－３を用いたルーチング情報を有しており、このルーチング情報に従って最適な経路を選択してパケットを転送する。例えば、中継ノード７－９は、パケットを受信した時に、受信パケット中の送信元アドレス４－２が示す端末アドレスと当該パケットを受信したポート、および、受信パケット中のＶＬＡＮ－ＩＤ４－３と当該パケットを受信したポートを対応づけて記憶する。次に、中継ノード７－９は、受信パケットがユニキャストパケットならば、宛先アドレス４－１が示す端末アドレスに対応するポートへ受信パケットを送信する。これに対し、受信パケットがブロードキャストパケット又はマルチキャストパケットならば、中継ノード７－９はＶＬＡＮ－ＩＤ４－３に対応する全てのポートへ受信パケットを送信する。なお、ここで言う"ポート"は、中継ノード７－９が自身に隣接する中継ノード又は無線基地局との間の通信路を接続するためのインタフェースである。また、中継路７－１０としては、図１に示した中継路１－１０と同様に各種のものが選択可能である。また、無線パケットバックボーン網７－５は中継ノード７－９を介して端末認証サーバ７－８に接続されている。端末認証サーバ７－８は図１に示した端末認証サーバ１－８と同じく表２に示した端末情報テーブルを記憶しており、無線パケット端末７－７が通信を開始する際に無線基地局７－６に対して端末情報を与える。

【００５０】本実施形態において、この端末情報テーブルに登録された暗号鍵は端末認証及びユニキャストパケットの暗号化に用いられ、以下ではこの暗号鍵を「端末鍵」という。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【００５１】以上に加えて、端末認証サーバ７－８は表３に示すＶＬＡＮ情報テーブルにＶＬＡＮ情報を持っている。

【００５２】

【表３】

第３の実施形態におけるVLAN情報テーブル

VLAN-ID	VLAN鍵
VLAN-ID#A	VLAN鍵#a
VLAN-ID#B	VLAN鍵#b

【００５３】このＶＬＡＮ情報テーブルは、ＶＬＡＮ－ＩＤと、同じＶＬＡＮ－ＩＤを持つ全ての端末で共通に使用する暗号鍵（以下、「ＶＬＡＮ鍵」という）との対応を記録している。このＶＬＡＮ鍵はブロードキャストパケット及びマルチキャストパケットの暗号化に使用される。なお、無線パケット網は各無線パケット端末７－７に対してＶＬＡＮ鍵をあらかじめ通知しておく。

【００５４】第１実施形態と同様に、ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【００５５】無線パケット端末７－７は自分の所属するユーザＬＡＮ７－４のＶＬＡＮ－ＩＤをそれぞれ端末認証サーバ７－８の端末情報テーブルにあらかじめ登録している。

【００５６】以下に詳述するように、無線基地局７－６は、無線パケット端末７－７から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザＬＡＮ７－４のＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し、何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００５７】本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【００５８】図９は、本実施形態におけるパケット転送手順を示している。第１実施形態と同様に、無線基地局７－６では、端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い、当該無線パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して、端末認証手段１０は端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得て端末情報記憶手段１１に記憶させる。一方、無線パケット端末７－７は、ユニキャストパケットを送信する時には端末鍵を選択して暗号化を行い、暗号化されたデータパケットを無線基地局７－６に送信する（８－１）。一方、無線パケット端末７－７は、ブロードキャストパケット又はマルチキャストパケットを送信する時にはＶＬＡＮ鍵を選択して暗号化を行い、暗号化されたデータパケットを無線基地局７－６に送信する（８－１）。これらに対応して、無線基地局７－６のパケット復号化手段１３は、ユニキャストパケットを受信した時には端末鍵を選択し

てデータパケットを復号し．また、ブロードキャストパケット又はマルチキャストパケットを受信した時にはＶＬＡＮ鍵を選択してデータパケットを復号する。パケット改竄検出手段１４は、図４に示した改竄検出手順に従って復号されたデータパケットの改竄の有無を調べ、改竄が検出された場合にはデータパケットを廃棄する。一方．データパケットの改竄が検出されない場合．端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、第２実施形態と同様にしてＶＬＡＮ－ＩＤ４－３と送信元アドレス４－２の対応を確認し、これらの対応が端末情報に登録済みであれば宛先アドレスで指定された宛先端末にデータパケットを転送する（８－２）。この時、本実施形態では．宛先端末がユーザＬＡＮ７－４と接続している場合．各中継ノード７－９はデータパケット中の宛先アドレス４－１に応じて次の送信ポートを選択してゲートウェイ７－３へデータパケットを転送する。ゲートウェイ７－３はＶＬＡＮ－ＩＤ４－３に応じてゲートウェイ７－１又はゲートウェイ７－２の何れかを選択してデータパケットをユーザＬＡＮ７－４に転送する。また．宛先端末が無線パケット網と接続している場合、各中継ノード７－９は宛先アドレス４－１に応じて次の送信ポートを選択してデータパケットを宛先端末へ転送する。したがってこの場合はゲートウェイを介することなくデータパケットが転送される。一方、ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段１６はデータパケットを廃棄する。

【００５９】図１０は、本実施形態におけるブロードキャストパケットの転送手順を示している。送信元端末ではデータが生起するとブロードキャストパケットを無線基地局７－６に送信する（９－１）．無線基地局７－６では．パケット暗号化手段１２が端末認証手段１０から取得した暗号鍵のうちＶＬＡＮ鍵を選択（９－２）してブロードキャストパケットを暗号化（９－３）し．全てのパケット端末（同図では無線パケット端末＃１．＃２）へブロードキャストパケットを送信する（９－４）。各無線パケット端末＃１，＃２では、暗号鍵としてＶＬＡＮ鍵を選択（９－５）し、暗号化されたブロードキャストパケットを復号化する（９－６）。このように本実施形態では、暗号化にＶＬＡＮ鍵を用いているため．同じＶＬＡＮ－ＩＤを有するパケット端末がブロードキャストパケット及びマルチキャストパケットを復号化することが可能である。

【００６０】図１１は、ブロードキャストパケットがネットワーク内を転送されてゆく様子を示している。同図に示すように．ユーザＬＡＮ＃Ａに属する無線パケット端末７－７ａ（送信端末）がブロードキャストパケットを無線基地局７－６ａに送信すると．このパケットは無線パケットバックボーン網７－５に送出される。無線パケットバックボーン網７－５は、ＶＬＡＮ－ＩＤ４－３に応じて中継ノード７－９ａからゲートウェイ７－３及び中継ノード７－９ｂにブロードキャストパケットを転送する。ここで．ゲートウェイ７－３はＶＬＡＮ－ＩＤ４－３を見て．ユーザＬＡＮ＃Ａに接続されたゲートウェイ７－１へブロードキャストパケットを転送する。一方．中継ノード７－９ｂはブロードキャストパケットをさらに中継ノード７－９ｃと転送し．中継ノード７－９ｃは．ユーザＬＡＮ＃Ａに属する無線パケット端末７－７ｃが接続された無線基地局７－６ｃにブロードキャストパケットを転送する。

【００６１】このように．ＶＬＡＮ－ＩＤを用いたルーチング情報によって経路が選択されてブロードキャストパケットが転送される。また、無線基地局７－６ｂにはユーザＬＡＮ＃Ｂに属する無線パケット端末７－７ｂのみが接続されており、ＶＬＡＮ－ＩＤ４－３と同じＶＬＡＮ－ＩＤを有する無線パケット端末を配下に持っていない。したがって、中継ノード７－９ｂは無線基地局７－６ｂに対してブロードキャストパケットを転送しない。

【００６２】なお、上述した説明では第２実施形態を基にしたパケット転送手順について説明したが、第１実施形態を基にしても良い。そうした場合．端末情報テーブルとしては表２の代わりに表１を使用することになるほか．ＶＬＡＮ－ＩＤと送信元アドレスの対応が端末情報に登録済みであるか確認する（図９における８－３）代わりに、この対応が端末情報に一致するかどうか確認することになる（図６における５－３）。

【００６３】以上のように．本実施形態によれば第１～第２実施形態に加えて以下の効果が得られる。すなわち．本実施形態では、宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には．ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【００６４】また、ブロードキャストパケット又はマルチキャストパケットを転送する場合は．ＶＬＡＮ－ＩＤに応じて次の中継ノードを選択して転送するため．同じＶＬＡＮ－ＩＤを用いて通信している全ての無線パケット端末に対してゲートウェイからユニキャスト転送する必要がない。したがって．最適な経路選択でパケットを転送することが可能であり．転送遅延時間，トラヒック、ゲートウェイの処理負荷の増加をそれぞれ防止することができる。

【００６５】また、ＶＬＡＮ－ＩＤが同じであれば共通の暗号鍵を用いてブロードキャストパケット又はマルチキャストパケットを暗号化しているため、無線基地局は．同一のＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して．１回の送信でブロードキャストパケット又はマルチキャストパケットを転送することが可能となる。したがって．各無線パケット端末の暗号鍵を用いて

暗号化したパケットを復数回送信する場合に比べて、トラヒック，転送遅延時間，基地局の負荷を抑制することができる。なお，ＶＬＡＮ鍵は端末固有の暗号鍵ではないが，異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【００６６】【第４実施形態】この第４実施形態は、請求項１，２，４，５，９記載のパケット転送方法および請求項１１，１４記載の基地局を適用した場合に相当している。

【００６７】本実施形態におけるパケット網のネットワーク構成は図８に示した第３実施形態の構成に等しい。また，本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【００６８】第３実施形態と同様に，ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【００６９】無線パケット端末７－７は、自分の所属するユーザＬＡＮ７－４のＶＬＡＮ－ＩＤをあらかじめ端末認証サーバ７－８の端末情報テーブルに登録している。

【００７０】第３実施形態と同様に，無線基地局７－６は，無線パケット端末７－７から受信したパケットの内，当該無線パケット端末が接続を許可されているユーザＬＡＮ７－４のＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し、何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００７１】また、端末認証サーバ７－８は表３に示した第３実施形態と同じＶＬＡＮ情報テーブルを持っており，ＶＬＡＮ鍵はブロードキャストパケット及びマルチキャストパケットの暗号化に使用される、無線パケット網が各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておくことも第３実施形態と同じである。

【００７２】本実施形態における端末情報テーブルは表２に示した第２実施形態の端末情報テーブルと等しい。この端末情報テーブルに登録された暗号鍵（端末鍵）は，端末認証時，ユニキャストパケットの暗号化時，ならびに，無線パケット端末によるブロードキャスト及びマルチキャストパケットの暗号化時にそれぞれ用いられる。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【００７３】図１２は、本実施形態におけるパケット転送手順を示している。無線基地局７－６では、第３実施形態と同様にして、端末認証手段１０が通信開始時において無線パケット端末７－７に対する認証を行い，当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に，第３実施形態とは異なって、無線パケット端末７－７はユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく端末鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１１－１），無線基地局７－６では、パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなく端末鍵を用いてデータパケットを復号化する。そしてこれ以後の手順は第３実施形態と同じである。無線基地局７－６は、受信したデータパケットが改竄されていればデータパケットを廃棄し，改竄されていなければＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録済みであれば宛先アドレス４－１で指定される宛先端末にデータパケットを転送する（１１－２）。このとき、データパケットは第３実施形態と同様に転送されてゆく。一方，ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段１６はデータパケットを廃棄する。

【００７４】本実施形態では、無線基地局７－６が送信するブロードキャストパケット及びマルチキャストパケットの暗号化の際には第３実施形態と同様にＶＬＡＮ鍵を用いるため，同じＶＬＡＮ－ＩＤを有するパケット端末はブロードキャストパケット及びマルチキャストパケットの復号が可能である。一方、無線パケット端末７－７が送信するブロードキャストパケット及びマルチキャストパケットの暗号化には端末鍵を用いているため、無線基地局７－６は第３実施形態のように２種類の暗号鍵（端末鍵，ＶＬＡＮ鍵）を切り替えて暗号を復号化する必要がない。

【００７５】また、本実施形態においてブロードキャストパケットをパケット網で転送する様子は、図１０～図１１に示す第３実施形態の場合に等しい。すなわち、無線基地局７－６がブロードキャスト又はマルチキャストパケットを送信する場合には、ＶＬＡＮ鍵を用いてパケットの暗号化が行われることになる。

【００７６】なお、上述した説明では第２実施形態を基にしたパケット転送手順について説明したが、第１実施形態を基にしても良い。その場合には，第３実施形態で説明したように，表１に示す端末情報テーブルを使用するとともに、ＶＬＡＮ－ＩＤと送信元アドレスの対応が端末情報に一致するかどうか確認することになる。

【００７７】以上のように，本実施形態によれば，第３実施形態と同様に、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【００７８】これに加えて本実施形態では、無線基地局がブロードキャストパケット又はマルチキャストパケッ

トを転送する際には、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化している。このため、無線基地局は同じＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して１回の送信でパケット転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。

【００７９】また、無線パケット端末がブロードキャストパケット又はマルチキャストパケットを転送する際、ユニキャストパケット用の暗号鍵を用いて暗号化している。したがって、無線基地局は無線パケット端末からパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となり、ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて、無線基地局にかかる負荷を抑制することができる。

【００８０】〔第５実施形態〕この第５実施形態は、請求項１，２，４，５，１０記載のパケット転送方法および請求項１１，１５記載の基地局を適用した場合に相当している。

【００８１】本実施形態におけるパケット網のネットワーク構成は、図８に示す第３実施形態の構成に等しい。また、本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【００８２】第３実施形態と同様に、ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【００８３】端末認証サーバ７－８は第３実施形態と同様に端末情報テーブル及びＶＬＡＮ情報テーブルを有している。

【００８４】第３実施形態と同様に、無線基地局７－６は、無線パケット端末７－７から受信したパケットの内、当該無線パケット端末が接続を許可されているユーザＬＡＮ７－４のＶＬＡＮ－ＩＤの何れかとＶＬＡＮ－ＩＤ４－３が一致するパケットのみを転送し、何れのＶＬＡＮ－ＩＤにも一致しないパケットは廃棄する。

【００８５】本実施形態では、ＶＬＡＮ鍵はパケットを暗号化するときに使用される。なお、無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【００８６】本実施形態における端末情報テーブルは、表２に示した第２実施形態の端末情報テーブルと等しい。ここで、本実施形態ではこの端末情報テーブルに登録する暗号鍵として、各パケット端末が所属するユーザＬＡＮ７－４のＶＬＡＮ鍵を用いる。

【００８７】図１３は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い、当該パケット端末が正規の端末であれば暗号通信を開始する。なお、この認証に際して端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、第３実施形態及び第４実施形態とは異なって、無線パケット端末７－７はユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なくＶＬＡＮ鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１２－１）。無線基地局７－６では、パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなくＶＬＡＮ鍵を用いてデータパケットを復号化する。そしてこれ以後の手順は第３実施形態と同じである。無線基地局７－６は、受信したデータパケットが改竄されていればパケットを廃棄し、改竄されていなければＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録済みであれば宛先アドレス４－１で指定される宛先端末にデータパケットを転送する（１２－２）。このとき、データパケットは第３実施形態と同様に転送されてゆく。一方、ＶＬＡＮ－ＩＤと送信元アドレスとの対応が端末情報に登録されていない場合、フィルタリング手段１６はデータパケットを廃棄する。

【００８８】本実施形態では、第３実施形態と違って暗号化にＶＬＡＮ鍵のみを用いるようにして端末鍵を用いてないため、同じＶＬＡＮ－ＩＤを有する無線パケット端末が、ブロードキャストパケット及びマルチキャストパケットに施された暗号を復号化することが可能である。また、無線基地局及び無線パケット端末は２種類の暗号鍵を切り替えて暗号化及び復号化を行う必要がないため、無線基地局及び無線パケット端末にかかる負荷を抑制することができる。

【００８９】なお、本実施形態においてブロードキャストパケットをパケット網で転送する様子は、図１１に示す第３実施形態の場合に等しい。また、上述した説明では第２実施形態を基にしたパケット転送手順について説明したが、第１実施形態を基にしても良い。その場合には、第３実施形態で説明したように、表１に示す端末情報テーブルを使用するとともに、ＶＬＡＮ－ＩＤと送信元アドレスの対応が端末情報に一致するかどうか確認することになる。

【００９０】以上のように、本実施形態によれば、第３実施形態と同様に、無線パケット端末が他の無線パケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって、転送遅延時間の増加を防止することができる。

【００９１】これに加えて本実施形態では、パケットを転送する際、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため、無線基地局は同じＶＬＡＮ－ＩＤを有する配下の全無線パケット端末に対して、１回の送

信でブロードキャストパケット及びマルチキャストパケットを転送することができる。したがって、各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック、転送遅延時間、基地局の負荷をそれぞれ抑制することができる。

【００９２】また、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いているため、無線基地局及び無線パケット端末はパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となる。したがって、２種類の暗号鍵を用いる場合に比べて、無線基地局及び無線パケット端末にかかる負荷を抑制することができる。なお、ＶＬＡＮ鍵は端末固有の暗号鍵ではないが、異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【００９３】【第６実施形態】この第６実施形態は、請求項１，３，５記載のパケット転送方法および請求項１２記載の基地局を適用した場合に相当している。本実施形態では第１実施形態に変形を加えて、ＶＬＡＮ－ＩＤを通信開始時において動的に割り当てるようにしたものである。本実施形態におけるパケット網のネットワーク構成、無線基地局の構成、データパケットの改竄検出手順及びパケットの信号フォーマットは、図１，図２，図４及び図５に示した第１実施形態の場合とそれぞれ等しい。

【００９４】本実施形態では、ＶＬＡＮ－ＩＤの動的割り当てを実現するためにユーザＬＡＮ１－４の各々にあらかじめ固有の名称（以下、「ユーザＬＡＮ名」という）を割り当てておく。例えば図１において、ＬＡＮ＃Ａには「ユーザＬＡＮ＃Ａ」を割り当て、ＬＡＮ＃Ｂには「ユーザＬＡＮ＃Ｂ」を割り当てるようにする。また、本実施形態ではユーザＬＡＮ名とＶＬＡＮ－ＩＤの対応関係を保持するために、無線基地局１－６が表４に示すＶＬＡＮ－ＩＤ割当管理テーブルを記憶している。さらに本実施形態において、端末認証サーバ１－８の保持する端末情報テーブルは表５に示す通りであり、ＶＬＡＮ－ＩＤの代わりにユーザＬＡＮ名を使用する点が第１実施形態（表１）と異なっている。

【００９５】

【表４】

VLAN-ID割当管理テーブル

ユーザLAN名	VLAN-ID
ユーザLAN#A	VLAN-ID#A
ユーザLAN#B	VLAN-ID#B
⋮	⋮

【００９６】

【表５】

端末情報テーブル

端末アドレス	ユーザLAN名	暗号鍵
アドレス#1	ユーザLAN#A	暗号鍵#a
アドレス#2	ユーザLAN#A	暗号鍵#b
アドレス#3	ユーザLAN#B	暗号鍵#c

【００９７】本実施形態では図３に示した認証手順に一部変更を加えて図１４に示す無線パケット端末の認証手順を採用している。図１４に示すように、無線パケット端末１－７は通信開始要求信号を無線基地局１－６へ送信する際に、自分の所属しているユーザＬＡＮに割り当てられたユーザＬＡＮ名（例えば「ユーザＬＡＮ＃Ａ」）を含めて送信している（１８－１）。無線基地局１－６では、端末認証手段１０が送られたユーザＬＡＮ名を内部に記憶しておく。次に、第１実施形態と同様に、無線基地局１－６は端末認証サーバ１－８に要求（２－２）を行って端末情報を取得（２－３）してこれを端末情報記憶手段１１に記憶し、端末認証用の乱数を暗号化して無線パケット端末１－７に認証要求信号を送信（２－４）し、無線パケット端末１－７が送り返す認証応答信号（２－５）に基づいて認証を行う。

【００９８】この認証によって無線パケット端末１－７が正規の端末と判断された場合、端末認証手段１０は無線パケット端末１－７から通知（１８－１）されているユーザＬＡＮ名にＶＬＡＮ－ＩＤを割り当てる（１８－６）。いま、無線パケット端末１－７から通知された例えばユーザＬＡＮ名が「ユーザＬＡＮ＃Ａ」である場合、端末認証手段１０はこのユーザＬＡＮに対して例えば「ＶＬＡＮ－ＩＤ＃Ａ」を割り当て、表４に示すように「ユーザＬＡＮ＃Ａ」および「ＶＬＡＮ－ＩＤ＃Ａ」の組をＶＬＡＮ－ＩＤ割当管理テーブルに追加する。次いで、端末認証手段１０は認証受付信号を用いて無線パケット端末１－７に通信許可を通知するが、このとき端末認証手段１０はいま割り当てたＶＬＡＮ－ＩＤ＃Ａを無線パケット端末１－７に通知する（１８－７）。なお、無線パケット端末１－７が不正端末と判断された場合の処理は第１実施形態と同じである。

【００９９】一方、図１５は本実施形態におけるパケット転送手順を示している。まず、本実施形態では認証手順として図１４に示した認証手順を実行する（１９－１）。次に、無線パケット端末１－７はデータパケットを無線基地局１－６に送信するが、その際、ＶＬＡＮ－ＩＤ４－３としては先に通知されたＶＬＡＮ－ＩＤ（図１４の１８－７）を用いる。この後は、第１実施形態と同様にして宛先端末へのデータパケットの転送（５－２）の処理までを行うが、データパケットが改竄されておらず、ユーザＬＡＮ名と送信元アドレスの対応が端末情報に一致するかどうか確認する際（１９－２）には次に述べる処理を行う。すなわち、無線基地局１－６では、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５が、送

信元アドレス４－２に対応するユーザＬＡＮ名を表５に示す端末情報テーブルから取得し、取得したユーザＬＡＮ名に対応するＶＬＡＮ－ＩＤを表４に示すＶＬＡＮ－ＩＤ割当管理テーブルから検索し、検索されたＶＬＡＮ－ＩＤとデータパケット中のＶＬＡＮ－ＩＤ４－３が一致するかどうか判定する。フィルタリング手段１６はこの判定結果に基づいて、両者が一致していれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送（５－２）し、両者が一致していなければデータパケットを廃棄する。その後に、無線パケット端末１－７と宛先端末との間で通信が終了したならば、無線基地局１－６では端末認証手段１０が表４に示したＶＬＡＮ－ＩＤ割当管理テーブルから「ユーザＬＡＮ＃Ａ」および「ＶＬＡＮ－ＩＤ＃Ａ」の組を削除しそれによって、無線パケット端末１－７に割り当てたＶＬＡＮ－ＩＤを解放する（１９－３）。

【０１００】以上のように、本実施形態では無線パケット端末１－７に対してＶＬＡＮ－ＩＤを動的に割り当てているため、限られたＶＬＡＮ－ＩＤを効率的に再利用＊

＊することができ、より多くのユーザＬＡＮを収容することができる。

【０１０１】［第７実施形態］この第７実施形態は、請求項１，３，５記載のパケット転送方法および請求項１２記載の基地局を適用した場合に相当している。本実施形態は、第６実施形態で説明したＶＬＡＮ－ＩＤの動的割り当てを第２実施形態に適用したものである。したがって、本実施形態におけるパケット網のネットワーク構成、無線基地局の構成，データパケットの改竄検出手順及びパケットの信号フォーマットは、図１，図２，図４及び図５に示した第１実施形態の場合とそれぞれ等しい。

【０１０２】本実施形態では、端末認証サーバ１－８が表６に示す端末情報テーブルを記憶している。表５（第６実施形態）と比較した場合、一つの端末アドレスについて、当該端末アドレスを持つパケット端末に通信を許可するユーザＬＡＮ名が複数登録されている。

【０１０３】

【表６】

端末情報テーブル

端末アドレス	ユーザLAN名	ユーザLAN名	暗号鍵
アドレス#1	ユーザLAN#A	ユーザLAN#B	暗号鍵#a
アドレス#2	ユーザLAN#A	ユーザLAN#B	暗号鍵#b
アドレス#3	ユーザLAN#B	－	暗号鍵#c

【０１０４】本実施形態における無線パケット端末の認証手順は図１６に示すものとなる。図１６に示す認証手順と図１４（第６実施形態）との相違は、無線パケット端末１－７が通信開始要求信号を無線基地局１－６へ送信する際に、通信相手のユーザＬＡＮ名を指定して無線基地局１－６に通知する（２０－１）点である。したがって、この後に行われる認証手順は第６実施形態と同じである。

【０１０５】一方、図１７は本実施形態におけるパケット転送手順を示している。本実施形態では、まず認証手順として図１６に示した手順を実行する（２１－１）。次に、無線パケット端末１－７はデータパケットを無線基地局１－６に送信するが、その際、ＶＬＡＮ－ＩＤ４－３としては先に通知されたＶＬＡＮ－ＩＤ（図１６の１８－７）を用いる。この後は、第２実施形態と同様にして宛先端末へのデータパケットの転送（６－２）の処理までを行うが、データパケットが改竄されておらず、ユーザＬＡＮ名と送信元アドレスの対応が端末情報に登録済みかどうか確認する際（２１－２）には次に述べる処理を行う。すなわち、無線基地局１－６において、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信パケットに含まれるＶＬＡＮ－ＩＤ４－３に対応するユーザＬＡＮ名を表４に示すＶＬＡＮ－ＩＤ割当管理テーブルから検索し、検索されたユーザＬＡＮ名と受信パケットに含まれる送信元アドレス４－２の組が、表６に示す端末情報テーブル中の端末アドレスとユーザＬＡＮ名の複数の組の中に存在するかどうかを調べ、この組が端末情報テーブルに存在していなければ上記対応が端末情報に未登録であると判断する。一方、この組が端末情報テーブルに存在する場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は当該ユーザＬＡＮ名に割り当ててあるＶＬＡＮ－ＩＤを表４に示すＶＬＡＮ－ＩＤ割当管理テーブルから取得し、取得したＶＬＡＮ－ＩＤとパケット中のＶＬＡＮ－ＩＤ４－３が一致するかどうか調べ、一致していれば上記対応が端末情報に登録済みであると判断し、一致していなければ上記対応が端末情報に未登録であると判断する。フィルタリング手段１６は、この判断結果に基づいて上記対応が端末情報に登録済みであれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送（６－２）し、上記対応が端末情報に未登録であればデータパケットを廃棄する。その後、無線パケット端末１－７と宛先端末の間で通信が終了したならば、第６実施形態と同様にして、端末認証手段１０は無線パケット端末１－７に割り当てたＶＬＡＮ－ＩＤを解放する（２１－３）。

【０１０６】［第８実施形態］この第８実施形態は、請求項１，２，５記載のパケット転送方法および請求項１１記載の基地局を適用した場合に相当している。これまで説明した各実施形態では、端末アドレスとしてＭＡＣアドレスを用い、ユーザＬＡＮに対してＶＬＡＮ－ＩＤ

を割り当てるようにしていた。これに対して、本実施形態では端末アドレスとしてＩＰアドレスを用いるとともに、ユーザＬＡＮには各ユーザＬＡＮ１－４に対して固有のネットワークアドレスをあらかじめ割り当てておく。前述したようにＩＰアドレスは図１８に示す構成をしているが、本実施形態ではこのＩＰアドレスに含まれるネットワークアドレス部をＶＬＡＮ－ＩＤの代わりに用いる。つまり、本実施形態においてはデータパケット中の宛先アドレス４－１の上位ビットを抽出することでネットワークアドレスが得られることになる。したがって、図５に示したＶＬＡＮ－ＩＤ４－３は不要となり、本実施形態における信号フォーマットは図１９に示すものとなる。

【０１０７】また、本実施形態における端末情報テーブルは表７に示すものとなり、表１で使用されていたＶＬＡＮ－ＩＤの代わりにネットワークアドレスが使用される。さらに、本実施形態における無線パケット端末１－７は、自分の所属するユーザＬＡＮ１－４のネットワークアドレスをそれぞれ端末認証サーバ１－８にあらかじめ登録している。なお、本実施形態におけるパケット網のネットワーク構成，，無線基地局の構成，無線パケット端末の認証手順及びデータパケットの改竄検出手順は、図１～図４に示した第１実施形態の場合とそれぞれ等しい。

【０１０８】

【表７】

端末情報テーブル

端末ｱﾄﾞﾚｽ	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#A	暗号鍵
ｱﾄﾞﾚｽ#1	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#A	暗号鍵#a
ｱﾄﾞﾚｽ#2	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#A	暗号鍵#b
ｱﾄﾞﾚｽ#3	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#B	暗号鍵#c

【０１０９】図２０は本実施形態におけるパケット転送手順を示しており、図６（第１実施形態）に示したパケット転送手順とは以下の点が相違する。すなわち、無線＊基地局１－６では、パケット改竄検出手段１４が受信したデータパケット（６－１）の改竄を検出しなかった場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信したデータパケットの宛先アドレス４－１からネットワークアドレス部を抽出し、送信元アドレス４－２に基

＊基づいて表７に示した端末情報テーブルから無線パケット端末１－７の所属するユーザＬＡＮのネットワークアドレスを取得して、これら２つのネットワークアドレスが一致するかどうかを確認する（２４－１）。その後、フィルタリング手段１６は送られた確認結果に基づいて、両ネットワークアドレスが一致していれば第１実施形態と同様に宛先アドレス４－１で指定された宛先端末にデータパケットを転送する（５－２）。一方、両ネットワークアドレスが一致していなければ、フィルタリング手段１６はデータパケットを廃棄する。

【０１１０】以上のように、本実施形態では、第１実施形態のようにデータパケット中にＶＬＡＮ－ＩＤのような余分なフィールドを設ける必要がない。

【０１１１】【第９実施形態】この第９実施形態は、請求項１，２，５記載のパケット転送方法および請求項１１記載の基地局を適用した場合に相当している。本実施形態は、第８実施形態で説明したネットワークアドレスの使用を第２実施形態に適用したものである。本実施形態においても、ユーザＬＡＮ１－４に対して各ユーザＬＡＮに固有のネットワークアドレスをあらかじめ割り当てておく。また、本実施形態における端末情報テーブルは表８に示す通りであって、表２で使用されていたＶＬＡＮ－ＩＤの代わりにネットワークアドレスが使用されている。なお、本実施形態におけるパケット網のネットワーク構成，無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図１～図４及び図１９に示したものとそれぞれ等しい。

【０１１２】

【表８】

端末情報テーブル

端末ｱﾄﾞﾚｽ	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ	暗号鍵
ｱﾄﾞﾚｽ#1	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#A	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#B	暗号鍵#a
ｱﾄﾞﾚｽ#2	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#A	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#D	暗号鍵#b
ｱﾄﾞﾚｽ#3	ﾈｯﾄﾜｰｸｱﾄﾞﾚｽ#B	－	暗号鍵#c

【０１１３】図２１は本実施形態におけるパケット転送手順を示しており、図７（第２実施形態）に示したパケット転送手順とは以下の点が相違する。すなわち、無線基地局１－６では、パケット改竄検出手段１４が受信したデータパケット（６－１）の改竄を検出しなかった場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信したデータパケットの宛先アドレス４－１からネットワークアドレス部を抽出し、送信元アドレス４－２に基づいて無線パケット端末１－７が通信を許されているユーザＬＡＮに割り当てられている全てのネットワークアドレスを表８に示した端末情報テーブルから取得する。次いで、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、取得したネットワークアドレスの中に宛先アドレス４－１から抽出されたネットワークアドレスと一致するものが登録されているかどうか確認する。フィルタリング手段１６は送られた確認結果に基づいて、一致するネ

ットワークアドレスが存在していれば宛先アドレス４－１で指定された宛先端末にデータパケットを転送（６－２）し、一致するネットワークが全く無ければデータパケットを廃棄する。

【０１１４】以上のように、本実施形態においても、第１実施形態のようにデータパケット中にＶＬＡＮ－ＩＤのような余分なフィールドを設ける必要がない。

【０１１５】［第１０実施形態］この第１０実施形態は、請求項１、２、４、５、８記載のパケット転送方法および請求項１１、１３記載の基地局を適用した場合に相当している。本実施形態は、第８実施形態で説明したネットワークアドレスの使用を第３実施形態に適用したものである。本実施形態においても、ユーザＬＡＮ１－４には各ユーザＬＡＮに固有のネットワークアドレスをあらかじめ割り当てておく。本実施形態におけるパケット網のネットワーク構成は図８に示した第３実施形態の場合と等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図４及び図１９に示したものとそれぞれ等しい。また、端末認証サーバ７－８には表９に示すＶＬＡＮ情報テーブルが設けられており、ＶＬＡＮ－ＩＤの代わりにネットワークアドレスを使用している点で表３（第３実施形態）と相違している。なお、本実施形態においても、第３実施形態と同様に、無線パケット網が各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１１６】

【表９】

VLAN情報テーブル

ネットワークアドレス	VLAN鍵
ネットワークアドレス #A	VLAN鍵#a
ネットワークアドレス #B	VLAN鍵#b

【０１１７】図２２は本実施形態におけるパケット転送手順を示しており、図９に示した第３実施形態の手順とは以下の点が相違する。まず、受信したデータパケット（８－１）の改竄が検出されなかった場合、第９実施形態と同様にして、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は、受信したデータパケットの宛先アドレス４－１から抽出されるネットワークアドレスが、無線パケット端末７－７に対して通信が許可されている複数のユーザＬＡＮ１－４に割り当てたネットワークアドレスの中に登録されているかどうかを確認する（２６－１）。そしてフィルタリング手段１６はこの確認結果に応じてパケットを転送する（８－２）か廃棄するかを決定する。

【０１１８】ここで、データパケットを転送する際（８－２）に、宛先端末がユーザＬＡＮ７－４と接続している場合、各中継ノード７－９はデータパケット中の宛先アドレス４－１に応じて次の送信ポートを選択してゲートウェイ７－３へデータパケットを転送する。ゲートウェイ７－３は宛先アドレス４－１から抽出されるネットワークアドレスに応じてゲートウェイ７－１又はゲートウェイ７－２を選択して、データパケットをユーザＬＡＮ７－４から宛先端末に転送する。一方、宛先端末が無線パケット網と接続している場合は、第３実施形態と同様に、各中継ノード７－９は宛先アドレス４－１に応じて次の送信ポートを選択して、ゲートウェイを介することなくパケットを宛先端末へ転送する。

【０１１９】本実施形態におけるブロードキャストパケットの転送手順は基本的に第３実施形態（図１０）と同様であって、ＶＬＡＮ－ＩＤの代わりに宛先アドレスから抽出されるネットワークアドレスを用いて経路選択が行われる点が相違している。

【０１２０】以上のように、本実施形態においても、第１実施形態のようにデータパケット中にＶＬＡＮ－ＩＤのような余分なフィールドを設ける必要がない。なお、ここではネットワークアドレスの使用を第３実施形態へ適用した場合について説明したが、第３実施形態と第４～第５実施形態とでは無線パケット端末７－７から無線基地局７－６へデータパケットを送信する際の暗号鍵の使い方が異なるだけである。したがって、これら第４～第５実施形態においてもＶＬＡＮ－ＩＤの代わりにネットワークアドレスを使用することができる。

【０１２１】［第１１実施形態］この第１１実施形態は、請求項１、６記載のパケット転送方法を適用した場合に相当している。

【０１２２】本実施形態におけるパケット網の構成、無線基地局の構成、無線パケット端末の認証手順及びデータパケットの改竄検出手順は、図１～図４に示した第１実施形態の場合とそれぞれ等しい。

【０１２３】表１０は、本実施形態における端末情報テーブルを示しており、端末アドレスと、端末認証に必要な情報としての暗号鍵とで構成されている。

【０１２４】

【表１０】

第１２実施形態における端末情報テーブル

端末アドレス	暗号鍵
アドレス#1	暗号鍵#a
アドレス#2	暗号鍵#b
アドレス#3	暗号鍵#c

【０１２５】各ユーザＬＡＮ１－４に接続するゲートウェイ１－１、１－２は、それぞれ許可アドレス情報を許可アドレステーブルに持っている。表１１はゲートウェイ１－１の許可アドレステーブルを示しており、表１２はゲートウェイ１－２の許可アドレステーブルを示している。ゲートウェイ１－１、１－２は、送信元アドレス４－２が各ゲートウェイの許可アドレステーブルに登録

されているデータパケットだけをユーザＬＡＮ１－４に転送する。

【０１２６】

【表１１】

ゲートウェイ1-1,7-1の許可アドレステーブル

許可ｱﾄﾞﾚｽ
ｱﾄﾞﾚｽ#1
ｱﾄﾞﾚｽ#2
－

【０１２７】

【表１２】

ゲートウェイ1-2,7-2の許可アドレステーブル

許可ｱﾄﾞﾚｽ
ｱﾄﾞﾚｽ#3
--
－

【０１２８】また、本実施形態における無線パケット網のパケットの信号フォーマットは、第８実施形態で説明した図１９のものと同じであって、宛先アドレス４－１と送信元アドレス４－２をヘッダ情報として持っており、ユーザデータ４－４は暗号化される。

【０１２９】図２３は、本実施形態におけるパケット転送手順を示している。無線基地局１－６では、端末認証手段１０が通信開始時に無線パケット端末１－７に対する認証を行い、当該パケット端末が正規の端末の場合は暗号通信を開始する。なお、この認証に際して端末認証手段１０は端末認証サーバ１－８から端末情報を得る。次に、無線パケット端末１－７は暗号化されたデータパケットを無線基地局１－６に送信する（１４－１）。無線基地局１－６ではパケット復号化手段１３がデータパケットを復号化して、パケット改竄検出手段１４が受信データパケット（１４－１）の改竄を検出した場合はこの受信データパケットを廃棄する。なお、これまでの手順は第１実施形態（図６）と同じである。一方、改竄が検出されない場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は第１実施形態のようにＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することはせず、受信データパケットをそのままフィルタリング手段１６に送出し、フィルタリング手段１６は宛先アドレス４－１で指定された宛先端末にデータパケットを転送する（１４－２）。この時、宛先端末がユーザＬＡＮ１－４と接続していれば、データパケットはゲートウェイ１－３からゲートウェイ１－１又はゲートウェイ１－２を介してユーザＬＡＮ１－４に転送される。その際、選択されたゲートウェイはデータパケット中の送信元アドレス４－２を確認し、当該アドレスが選択されたゲートウェイの許可

アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ１－４に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合、データパケットはゲートウェイを介することなく宛先端末に転送される。

【０１３０】以上のように、本実施形態では、通信開始時に端末認証することによって、無線パケット端末を特定可能であり、未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止することができる。また、暗号化してパケットを転送することにより、不正な端末が認証された正規の端末になりすますことを防止可能であり、なりすまし端末による不正アクセスを防止することができる。さらに、暗号の復号時に改竄を検出してパケットを廃棄することにより、改竄されたパケットの転送を防止可能であり、改竄データによる通信の妨害と無線パケット網のトラヒック増加を防止することができる。加えて、ゲートウェイが宛先アドレスと送信元アドレスに応じてパケットの転送を許可することで、認証されたパケット端末が通信の許可されていないユーザＬＡＮにアクセスするのを防止可能であり、他ユーザＬＡＮに所属している端末からの不正アクセスを防止することができる。

【０１３１】〔第１２実施形態〕この第１２実施形態は、請求項１、７、８記載のパケット転送方法を適用した場合に相当している。

【０１３２】本実施形態におけるパケット網の構成は図８に示す第３実施形態の構成に等しい。また、本実施形態における無線基地局の構成、無線パケット端末の認証手順、データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【０１３３】第３実施形態と同様に、ＶＬＡＮ－ＩＤは各ユーザＬＡＮ７－４に固有の値があらかじめ割り当てられている。

【０１３４】端末認証サーバ７－８は第３実施形態と同様に端末情報テーブルとＶＬＡＮ情報テーブルを有している。本実施形態におけるＶＬＡＮ情報テーブルは、表３に示す第３実施形態におけるＶＬＡＮ情報テーブルに等しい。本実施形態では、ＶＬＡＮ鍵がブロードキャストパケット及びマルチキャストパケットの暗号化に使用される。なお、無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１３５】本実施形態における端末情報テーブルは、表１０に示す第１１実施形態における情報テーブルと等しい。この端末情報テーブルに登録した暗号鍵（端末鍵）は、端末認証及びユニキャストパケットの暗号化に用いられる。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【０１３６】各ユーザＬＡＮ７－４に接続するゲートウェイ７－１，７－２は、第１１実施形態におけるゲート

ウェイ１－１，１－２と同様に、許可アドレス情報を表１１，表１２に示した許可アドレステーブルに持っている。

【０１３７】図２４は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い，当該パケット端末が正規の端末であれば暗号通信を開始する。なお，この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、無線パケット端末７－７は第３実施形態と同様にパケットに応じた暗号鍵としてＶＬＡＮ鍵又は端末鍵を選択し，暗号化されたデータパケットを無線基地局７－６に送信する（１５－１）。無線基地局７－６は第３実施形態と同様にパケットに応じた復号鍵を選択してデータパケットを復号化する。そして、パケット改竄検出手段１４が受信データパケット（１５－１）の改竄を検出した場合はこの受信データパケットを廃棄する。一方，改竄が検出されない場合、端末アドレス／ＶＬＡＮ－ＩＤ比較手段１５は第３実施形態のようにＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することはせず、受信データパケットをそのままフィルタリング手段１６に送出し、フィルタリング手段１６は宛先アドレス４－１で指定される宛先端末に転送するためにデータパケットを無線パケット網へ送信する（１５－２）。この時，宛先端末がユーザＬＡＮ７－４と接続している場合，各中継ノード７－９はデータパケット中の宛先アドレス４－１に応じて次の送信ポートを選択してゲートウェイ７－３へデータパケットを転送する。ゲートウェイ７－３は宛先アドレス４－１から抽出されるネットワークアドレスに応じてゲートウェイ７－１又はゲートウェイ７－２を選択し，選択されたゲートウェイに接続するユーザＬＡＮ７－４から宛先端末にデータパケットを転送する（１５－３）。その際，選択されたゲートウェイはデータパケット中の送信元アドレス４－２を確認し、当該アドレスが選択されたゲートウェイの許可アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ７－４に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合は，第３実施形態と同様に，各中継ノード７－９は宛先アドレス４－１に応じて次の送信ポートを選択して、ゲートウェイを介することなくデータパケットを宛先端末へ転送する。

【０１３８】本実施形態におけるブロードキャストパケットの転送手順は、図１０に示す第３実施形態の場合と等しい。本実施形態では，暗号化にＶＬＡＮ鍵を用いているため、第３実施形態と同様に、ＶＬＡＮ－ＩＤの同じパケット端末は、ブロードキャストパケット及びマルチキャストパケットの復号が可能である。

【０１３９】また，本実施形態においてブロードキャストパケットをパケット網が転送する様子は、図１１に示す第３実施形態の場合と等しい。

【０１４０】以上のように，本実施形態によれば，第１１実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち，宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には，ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって，転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、ＶＬＡＮ－ＩＤにより次の中継ノードを選択してパケットを転送するため、同じＶＬＡＮ－ＩＤを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり，最適な経路選択で転送することが可能であって，転送遅延時間，トラヒック，ゲートウェイの処理負荷の増加を防止することができる。また、ブロードキャストパケット又はマルチキャストパケットを転送する際は、ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため，無線基地局は同じＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して１回の送信でこれらパケットを転送することができる。したがって，各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて，トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制することができる。なお，ＶＬＡＮ鍵は端末固有の暗号鍵ではないが，異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【０１４１】〔第１３実施形態〕この第１３実施形態は，請求項１，７，９記載のパケット転送方法を適用した場合に相当している。

【０１４２】本実施形態におけるパケット網の構成は図８に示す第３実施形態の構成に等しい。また、本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは、図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【０１４３】第３実施形態と同様に，ＶＬＡＮ－ＩＤは各ユーザＬＡＮに固有の値があらかじめ割り当てられている。端末認証サーバ７－８は第３実施形態と同様に端末情報テーブルとＶＬＡＮ情報テーブルを有している。本実施形態におけるＶＬＡＮ情報テーブルは、表３に示す第３実施形態におけるＶＬＡＮ情報テーブルに等しい。

【０１４４】本実施形態において、ＶＬＡＮ鍵は無線基地局７－６がブロードキャストパケット及びマルチキャストパケットを暗号化するときに使用される。なお、無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１４５】また、本実施形態における端末情報テーブ

ルは表１０に示す第１１実施形態の端末情報テーブルと等しい。この端末情報テーブルに登録した暗号鍵（端末鍵）は、端末認証時，ユニキャストパケットの暗号化時，ならびに，無線パケット端末７－７によるブロードキャスト及びマルチキャストパケットの暗号化時においてそれぞれ用いられる。なお、無線パケット網は各無線パケット端末７－７に端末鍵をあらかじめ通知しておく。

【０１４６】ゲートウェイ７－１，７－２は第１１実施形態におけるゲートウェイ１－１，１－２と同様に、表１１，表１２に示す許可アドレステーブルをそれぞれ有している。

【０１４７】図２５は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い，当該パケット端末が正規の端末であれば暗号通信を開始する。なお，この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、無線パケット端末７－７は第４実施形態と同様にユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なく端末鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１６－１）。無線基地局７－６では、パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなく端末鍵を用いてデータパケットを復号化する。これ以後は，第１２実施形態と同様に、無線基地局７－６は受信したデータパケットが改竄されていればパケットを廃棄し，改竄されていない場合は、ＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することなく、第１２実施形態と同様にして宛先アドレス４－１で指定される宛先端末までデータパケットを転送する（１６－３）。すなわち，宛先端末がユーザＬＡＮ７－４と接続しているならば，データパケットは各中継ノード７－９，ゲートウェイ７－３，ゲートウェイ７－１又はゲートウェイ７－２，ユーザＬＡＮ７－４を経て宛先端末に転送される。その際，ゲートウェイ７－１又は７－２はデータパケット（１６－２）の送信元アドレス４－２が許可アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ７－４に転送し，未登録であれば当該データパケットを廃棄する。一方，宛先端末が無線パケット網と接続している場合，データパケットはゲートウェイを介することなく宛先端末へ転送される。

【０１４８】また，本実施形態においてブロードキャストパケットをパケット網が転送する様子は図１１に示す第３実施形態の場合に等しい。

【０１４９】本実施形態によれば，第１１実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち，宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため，無線パケット端末が他の無線パケット端末にパケット転送する時には，ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって，転送遅延時間の増加を防止することができる。また，ブロードキャストパケット及びマルチキャストパケットを転送する場合は，ＶＬＡＮ－ＩＤにより次の中継ノードを選択してパケットを転送するため，同じＶＬＡＮ－ＩＤを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり，最適な経路選択で転送することが可能であって，転送遅延時間，トラヒック，ゲートウェイの処理負荷の増加を防止することができる。また，無線基地局が送信するブロードキャストパケット及びマルチキャストパケットの暗号化の際にはＶＬＡＮ鍵を用いるため，ＶＬＡＮ－ＩＤの同じパケット端末は暗号の復号が可能である。また，無線基地局がブロードキャストパケット又はマルチキャストパケットを転送する際は，ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため，無線基地局は同じＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して１回の送信でこれらパケットを転送することができる。したがって，各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて，トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制することができる。さらに，無線パケット端末は，送信するブロードキャストパケット及びマルチキャストパケットの暗号化に際して、ユニキャストパケット用の暗号鍵である端末鍵を用いている。そのため、第１２実施形態などとは異なり、無線基地局はパケットの受信時に２種類の暗号鍵を切り替えることなく暗号を復号することが可能となる。したがって，ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて，無線基地局の負荷を抑制することができる。

【０１５０】〔第１４実施形態〕この第１４実施形態は，請求項１，７，１０記載のパケット転送方法を適用した場合に相当している。

【０１５１】本実施形態におけるパケット網の構成は図８に示す第３実施形態の構成に等しい。また，本実施形態における無線基地局の構成，無線パケット端末の認証手順，データパケットの改竄検出手順及びパケットの信号フォーマットは，図２～図５に示した第１実施形態の場合とそれぞれ等しい。

【０１５２】第３実施形態と同様に，ＶＬＡＮ－ＩＤは各ユーザＬＡＮに対して固有の値があらかじめ割り当てられている。端末認証サーバ７－８は第３実施形態と同様に端末情報テーブルとＶＬＡＮ情報テーブルを有している。本実施形態におけるＶＬＡＮ情報テーブルは，表３に示す第３実施形態におけるＶＬＡＮ情報テーブルに等しい。本実施形態では，第５実施形態と同様に，ＶＬＡＮ鍵はパケットを暗号化するときに使用される。な

お．無線パケット網は各無線パケット端末７－７にＶＬＡＮ鍵をあらかじめ通知しておく。

【０１５３】本実施形態における端末情報テーブルは表１０に示した第１１実施形態の端末情報テーブルと等しい。また、端末情報テーブルに登録した暗号鍵としては．各端末が所属するユーザＬＡＮ７－４のＶＬＡＮ鍵を用いる。

【０１５４】ゲートウェイ７－１，７－２は第１１実施形態におけるゲートウェイ１－１，１－２と同様に、それぞれ表１１．表１２に示す許可アドレステーブルを有している。

【０１５５】図２６は、本実施形態におけるパケット転送手順を示している。第３実施形態と同様に、無線基地局７－６では端末認証手段１０が通信開始時に無線パケット端末７－７に対する認証を行い．当該パケット端末が正規の端末であれば暗号通信を開始する。なお．この認証に際して端末認証手段１０が端末認証サーバ７－８から端末情報と共にＶＬＡＮ情報を得るのも第３実施形態と同じである。次に、無線パケット端末７－７は第５実施形態と同様にユニキャストパケット／ブロードキャストパケット／マルチキャストパケットの区別なくＶＬＡＮ鍵を用いてデータパケットを暗号化して無線基地局７－６に送信する（１７－１）。無線基地局７－６では．パケット復号化手段１３がユニキャストパケット／ブロードキャストパケット／マルチキャストパケットを区別することなくＶＬＡＮ鍵を用いてデータパケットを復号化する。これ以後は．第１２実施形態と同様に、無線基地局７－６は受信したデータパケットが改竄されていればパケットを廃棄し．改竄されていない場合は、ＶＬＡＮ－ＩＤと送信元アドレスとの対応を確認することなく．第１２実施形態と同様にして宛先アドレス４－１で指定される宛先端末までデータパケットを転送する（１７－３）。すなわち．宛先端末がユーザＬＡＮ７－４と接続しているならば．データパケットは各中継ノード７－９，ゲートウェイ７－３，ゲートウェイ７－１又はゲートウェイ７－２，ユーザＬＡＮ７－４を経て宛先端末に転送される。その際．ゲートウェイ７－１又は７－２はデータパケット（１７－２）の送信元アドレス４－２が許可アドレステーブルに登録済みであればデータパケットをユーザＬＡＮ７－４に転送し、未登録であれば当該データパケットを廃棄する。一方、宛先端末が無線パケット網と接続している場合，データパケットはゲートウェイを介することなく宛先端末へ転送される。

【０１５６】本実施形態においてブロードキャストパケットをパケット網が転送する様子は．図１１に示す第３実施形態の場合と等しい。

【０１５７】以上のように．本実施形態によれば．第１１実施形態によって得られる効果に加えて次に述べる効果が得られる。すなわち．宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、無線パケット端末が他の無線パケット端末にパケット転送する時には．ゲートウェイを経由することなく最適な経路を選択して転送することが可能であって．転送遅延時間の増加を防止することができる。また、ブロードキャストパケット及びマルチキャストパケットを転送する場合は、ＶＬＡＮ－ＩＤにより次の中継ノードを選択してパケットを転送するため、同じＶＬＡＮ－ＩＤを用いて通信中の全ての無線パケット端末に対してゲートウェイがユニキャスト転送する必要がなくなり、最適な経路選択で転送することが可能であって．転送遅延時間，トラヒック．ゲートウェイの処理負荷の増加を防止することができる。また、本実施形態では、暗号化にＶＬＡＮ鍵のみを用いるようにして端末鍵を用いないため、ＶＬＡＮ－ＩＤの同じパケット端末はブロードキャスト及びマルチキャストパケットの暗号を復号することが可能である。また．ＶＬＡＮ－ＩＤに共通する暗号鍵を用いているため．無線基地局及び無線パケット端末はパケット受信時に２種類の暗号鍵を切り替えて暗号化及び復号する必要がない。したがって、２種類の暗号鍵を用いる場合に比べて．無線基地局及び無線パケット端末の負荷を抑制することができる。また、パケットを転送する際は．ＶＬＡＮ－ＩＤに共通する暗号鍵を用いて暗号化しているため．無線基地局は同じＶＬＡＮ－ＩＤを持つ配下の全無線パケット端末に対して１回の送信でこれらパケットを転送することができる。したがって．各無線パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて．トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制することができる。なお、ＶＬＡＮ鍵は端末固有の暗号鍵ではないが、異なるＶＬＡＮ－ＩＤを持つパケット端末は知りえないため、なりすましによる不正アクセスは生じない。

【０１５８】［第１５実施形態］上述した各実施形態では本発明を無線パケット網へ適用した場合について説明してきたが、本発明は無線パケット網に限らず有線パケット網に適用しても良い。図２７は．前述した第１実施形態を有線パケット網で実現した場合のネットワーク構成を示している。同図では．無線パケットバックボーン網１－５と同等の機能を有するパケットバックボーン網２７－５，無線／有線の違いを除いて無線基地局１－６と同等の機能を有するアクセスサーバ（有線接続装置）２７－６，および無線／有線の違いを除いて無線パケット端末１－７と同等の機能を有するパケット端末２７－７がそれぞれ設けられている。これら以外の構成は全て第１実施形態（図１）と同じである。本実施形態によるパケット転送手順は、アクセスサーバ２７－６とパケット端末２７－７の間を含めた全ての通信が有線で行われる点を除けば．第１実施形態と全く同じになる。また、図８に示したネットワーク構成を用いる場合にも．無線パケットバックボーン網７－５，無線基地局７－６，無線パケット端末７－７をそれぞれパケットバックボーン

網２７－５，アクセスサーバ２７－６，パケット端末２７－７に置き換えれば良い。したがって、上述した全ての実施形態に対して有線パケット網のネットワーク構成を適用することができる。

【０１５９】以上述べた実施形態は全て本発明を例示的に示すものであって限定的に示すものではなく，本発明は他の種々の変形態様及び変更態様で実施することができる。従って本発明の範囲は特許請求の範囲及びその均等範囲によってのみ規定されるものである。

【０１６０】例えば、上記各実施形態では、パケット網への入口である無線基地局（あるいはアクセスサーバ）が端末認証やパケット改竄検出などを行うことによって，最も効率的な転送を実現することができる。しかしながら、パケット網の構成によっては無線基地局を統括する制御局などが設けられている場合もあり、そうした場合には、この制御局が端末認証やパケット改竄検出を行うようにしても良い。

【０１６１】

【発明の効果】以上説明したように，本発明によれば、通信開始時に端末認証することによってパケット端末を特定可能であり，未知の端末や端末アドレスを偽造した端末からの不正アクセスを防止する効果が得られる。また，暗号化してパケットを転送することにより，不正な端末が認証された正規の端末になりすますことを防止可能であり、なりすまし端末による不正アクセスを防止する効果が得られる。さらに，暗号の復号時に改竄を検出してパケットを廃棄することにより，改竄されたパケットの転送を防止可能であり，改竄データによる通信の妨害とパケット網のトラヒック増加を防止する効果が得られる。

【０１６２】従って、送信元アドレスを偽造することによりデータ網（ユーザＬＡＮ）へ不正にアクセスできる問題を解決し，あらかじめ登録した端末に対してだけ特定のデータ網との通信を許可するパケット転送方法を提供することが可能となる。また、パケットの転送遅延時間，トラヒック，ゲートウェイの負荷が増加する問題を解決し、最適な経路選択が可能でなおかつ効率的なパケット転送方法を提供することが可能となる。

【０１６３】また、請求項２，３，１１又は１２記載の発明によれば，識別子又はユーザＬＡＮ名と送信元アドレスの対応を確認することにより、認証された端末が自分が接続の許可されていない（あるいは自分の属していない）データ網にアクセスすることを防止可能であり、あるデータ網に接続を許可されている（あるいは所属している）端末から他データ網への不正アクセスを防止する効果が得られる。さらにまた、１パケット端末あたり複数の識別子又はユーザＬＡＮ名を登録することにより，１つのパケット端末で複数のデータ網にアクセスすることが可能であり、ユーザへのサービス性が向上するという効果が得られる。

【０１６４】また、請求項４又は７記載の発明によれば，宛先アドレスに応じて次の中継ノードを選択してパケットを転送するため、パケット端末が他のパケット端末にパケット転送する時には、ゲートウェイを経由することなく最適な経路を選択して転送することが可能であり，転送遅延時間の増加を防止する効果が得られる。また，ブロードキャストパケット及びマルチキャストパケットを転送する場合は、識別子に応じて次の中継ノードを選択してパケットを転送するため，同じ識別子を用いて通信している全てのパケット端末に対してゲートウェイからユニキャスト転送する必要がない。したがって、最適な経路選択でパケットを転送することが可能であり，転送遅延時間，トラヒック，ゲートウェイの処理負荷の増加をそれぞれ防止する効果が得られる。

【０１６５】また、請求項６記載の発明によれば，ゲートウェイが宛先アドレスと送信元アドレスに応じてパケットの転送を許可することで、認証されたパケット端末が通信の許可されていないユーザＬＡＮにアクセスすることを防止可能であり、他ユーザＬＡＮに所属しているパケット端末からの不正アクセスを防止する効果が得られる。

【０１６６】また、請求項８又は１３記載の発明によれば，識別子が同じであれば共通の暗号鍵を用いてブロードキャストパケット及びマルチキャストパケットを暗号化しているため，基地局は同一の識別子を持つ配下の全パケット端末に対して１回の送信でこれらパケットを転送することが可能となる。したがって，各パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて，トラヒック，転送遅延時間，基地局の負荷を抑制する効果が得られる。

【０１６７】また、請求項９又は１４記載の発明によれば，基地局がブロードキャストパケット及びマルチキャストパケットを転送する際には、識別子に共通する暗号鍵を用いて暗号化している。このため，基地局は同じ識別子を持つ配下の全パケット端末に対して１回の送信でこれらパケットを転送することが可能となる。したがって，各パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて，トラヒック，転送遅延時間，基地局の負荷をそれぞれ抑制する効果が得られる。また、パケット端末がブロードキャストパケット及びマルチキャストパケットを転送する際には、ユニキャストパケット用の暗号鍵を用いて暗号化している。したがって，基地局はパケット端末からパケットを受信した時に暗号鍵を切り替えることなく復号することが可能となり，ブロードキャストパケット及びマルチキャストパケット用の暗号鍵を用いて暗号化して送信する場合に比べて，基地局にかかる負荷を抑制する効果が得られる。

【０１６８】また、請求項１０又は１５記載の発明によれば，パケットを転送する際、識別子に共通の暗号鍵を用いて暗号化しているため，基地局は同じ識別子を有す

る配下の全パケット端末に対して１回の送信でブロードキャストパケット及びマルチキャストパケットを転送することが可能となる。したがって、各パケット端末の暗号鍵を用いて暗号化して複数回送信する場合に比べて、トラヒック，転送遅延時間、基地局の負荷をそれぞれ抑制する効果が得られる。また、識別子に共通する暗号鍵を用いているため、基地局及びパケット端末はパケットの受信時において暗号鍵を切り替えることなく復号することが可能となる。したがって、２種類の暗号鍵を用いる場合に比べて，基地局及びパケット端末にかかる負荷を抑制する効果が得られる。

【図面の簡単な説明】

【図１】　本発明の第１実施形態における無線パケット通信のネットワーク構成を示すブロック図である。

【図２】　本発明の各実施形態における無線基地局の構成を示すブロック図である。

【図３】　本発明の第１実施形態における無線パケット通信の認証手順を示す図である。

【図４】　同実施形態におけるデータパケットの改竄検出手順を示す図である。

【図５】　同実施形態におけるパケットの信号フォーマットを示す図である。

【図６】　同実施形態におけるパケット転送手順を示す図である。

【図７】　本発明の第２実施形態におけるパケット転送手順を示す図である。

【図８】　本発明の第３実施形態における無線パケット通信のネットワーク構成を示すブロック図である。

【図９】　同実施形態におけるパケット転送手順を示す図である。

【図１０】　同実施形態におけるブロードキャストパケットの転送手順を示す図である。

【図１１】　同実施形態におけるブロードキャストパケットの転送の様子を示す図である。

【図１２】　本発明の第４実施形態におけるパケット転送手順を示す図である。

【図１３】　本発明の第５実施形態におけるパケット転送手順を示す図である。

【図１４】　本発明の第６実施形態における無線パケット通信の認証手順を示す図である。

【図１５】　同実施形態におけるパケット転送手順を示す図である。

【図１６】　本発明の第７実施形態における無線パケット通信の認証手順を示す図である。

【図１７】　同実施形態におけるパケット転送手順を示す図である。

【図１８】　ＩＰアドレスの構成を示す図である。

【図１９】　本発明の第８実施形態におけるパケットの信号フォーマットを示す図である。

【図２０】　同実施形態におけるパケット転送手順を示す図である。

【図２１】　本発明の第９実施形態におけるパケット転送手順を示す図である。

【図２２】　本発明の第１０実施形態におけるパケット転送手順を示す図である。

【図２３】　本発明の第１１実施形態におけるパケット転送手順を示す図である。

【図２４】　本発明の第１２実施形態におけるパケット転送手順を示す図である。

【図２５】　本発明の第１３実施形態におけるパケット転送手順を示す図である。

【図２６】　本発明の第１４実施形態におけるパケット転送手順を示す図である。

【図２７】　本発明の第１５実施形態における有線パケット通信のネットワーク構成を示すブロック図である。

【符号の説明】

１－１、１－２．１－３．７－１、７－２、７－３　ゲートウェイ

１－４、７－４　ユーザＬＡＮ

１－５、７－５　無線パケットバックボーン網

１－６、７－６．７－６ａ～７－６ｃ　無線基地局

１－７、７－７．７－７ａ～７－７ｃ　無線パケット端末

１－８、７－８　端末認証サーバ

１－１０、７－１０　中継路

４－１　宛先アドレス

４－２　送信元アドレス

４－３　ＶＬＡＮ－ＩＤ

４－４　ユーザデータ

７－９、７－９ａ～７－９ｃ　中継ノード

１０　端末認証手段

１１　端末情報記憶手段

１２　パケット暗号化手段

１３　パケット復号化手段

１４　パケット改竄検出手段

１５　端末アドレス／ＶＬＡＮ－ＩＤ比較手段

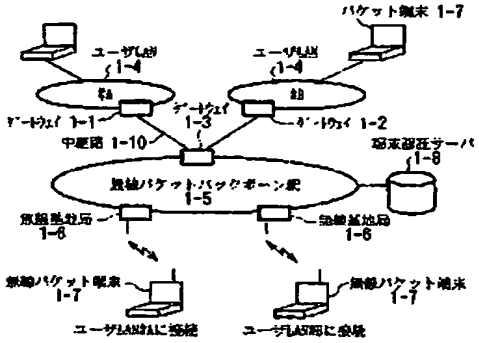
１６　フィルタリング手段

２７－５　パケットバックボーン網

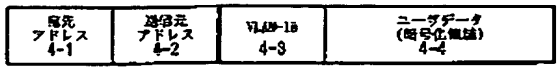
２７－６　アクセスサーバ（有線接続装置）

２７－７　パケット端末

【図１】

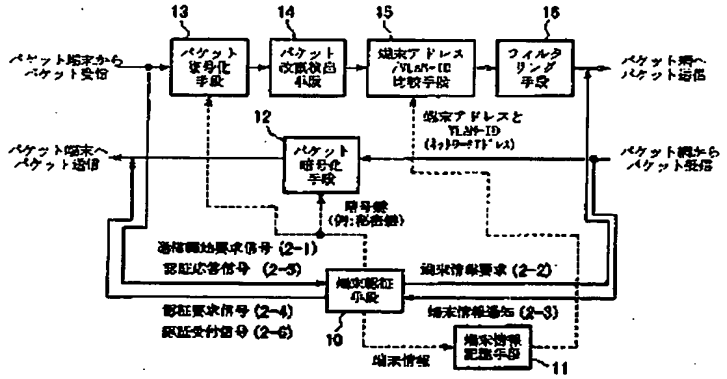


【図５】

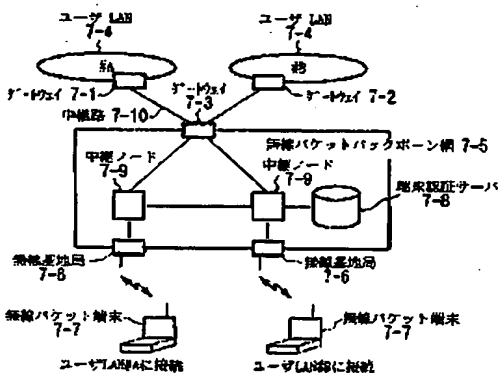


【図１８】

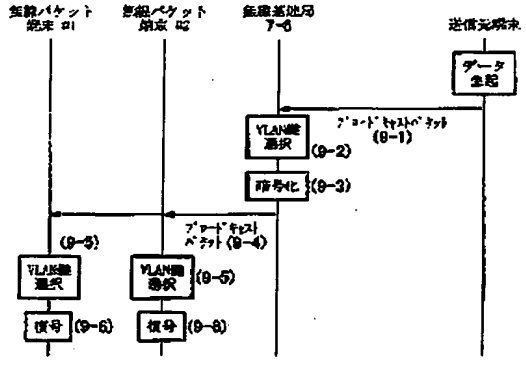
【図２】



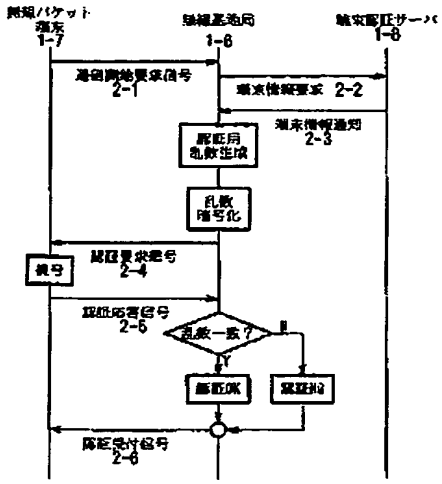
【図８】



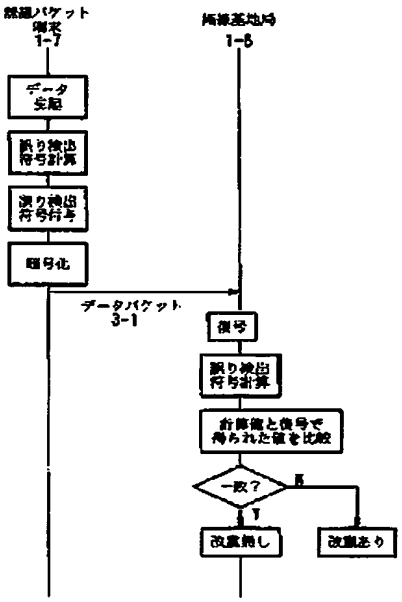
【図１０】



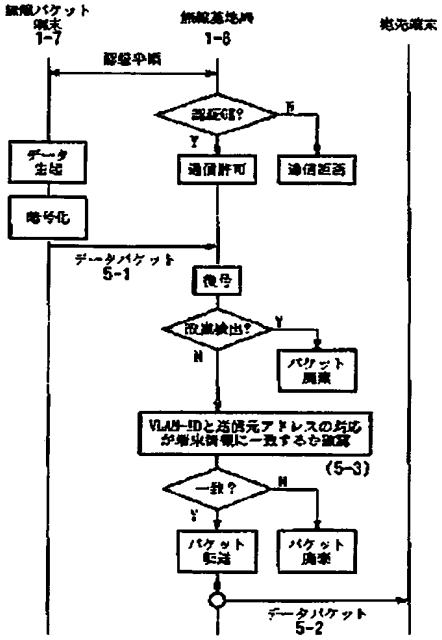
【図３】


無線パケット端末 1-7
無線基地局 1-6
端末認証サーバ 1-8
通信開始要求信号 2-1
端末情報要求 2-2
端末情報通知 2-3
認証用乱数生成
乱数暗号化
応答
認証要求信号 2-4
認証応答信号 2-5
乱数一致？
N
Y
認証OK
認証NG
認証受付信号 2-6

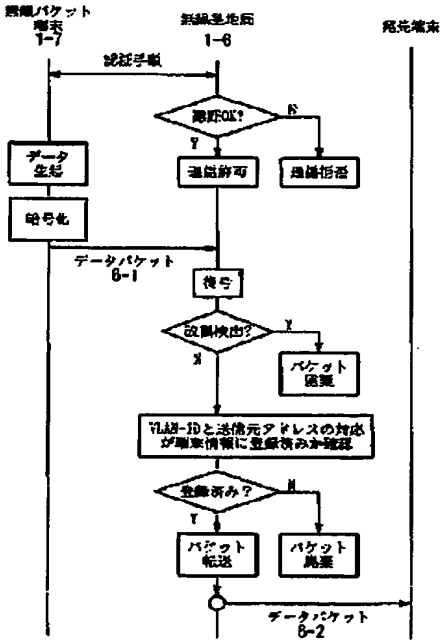
【図４】


無線パケット端末 1-7
無線基地局 1-8
データ生起
誤り検出符号計算
誤り検出符号付与
暗号化
データパケット 3-1
復号
誤り検出符号計算
計算値と復号で得られた値を比較
一致？
N
Y
改竄無し
改竄あり

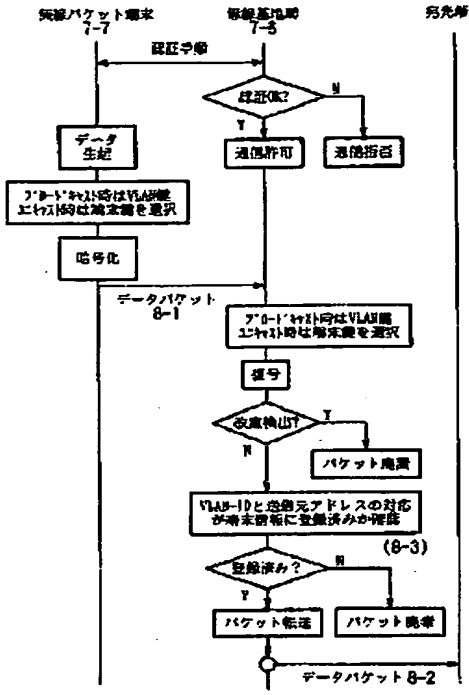
【図６】


無線パケット端末 1-7
無線基地局 1-8
宛先端末
認証手順
認証OK?
N
Y
データ生起
通信許可
通信拒否
暗号化
データパケット 5-1
復号
改竄検出?
Y
N
パケット廃棄
VLAN-IDと送信元アドレスの対応が端末情報に一致するか確認
(5-3)
一致？
N
Y
パケット転送
パケット廃棄
データパケット 5-2

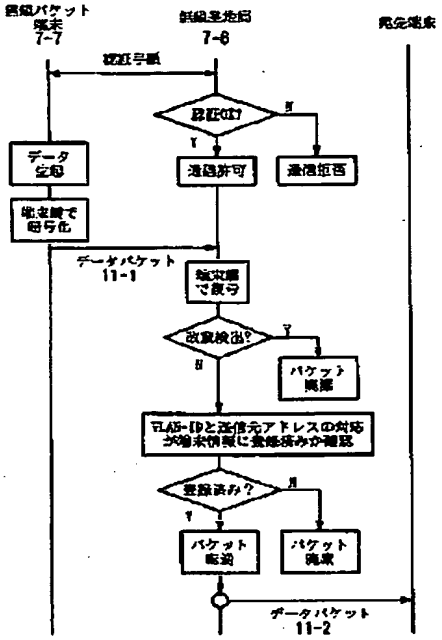
【図７】


無線パケット端末 1-7
無線基地局 1-6
宛先端末
認証手順
認証OK?
N
Y
データ生起
通信許可
通信拒否
暗号化
データパケット 6-1
復号
改竄検出?
Y
N
パケット廃棄
VLAN-IDと送信元アドレスの対応が端末情報に登録済みか確認
登録済み？
N
Y
パケット転送
パケット廃棄
データパケット 6-2

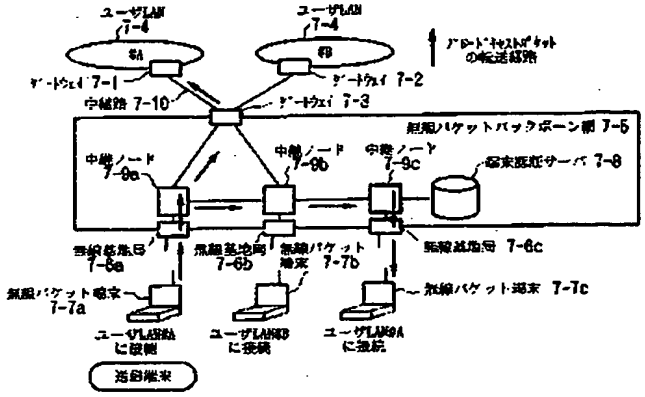
【図９】



【図１２】



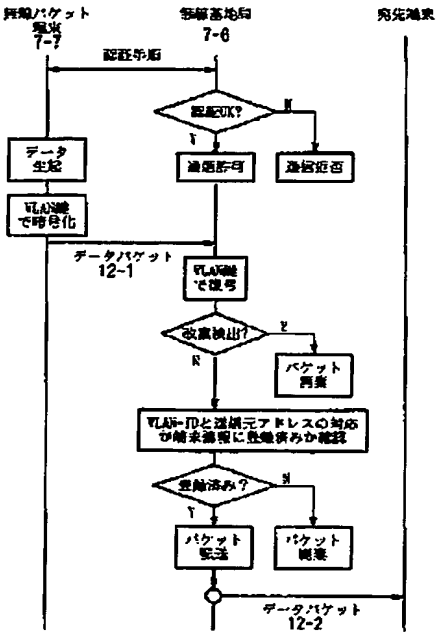
【図１１】



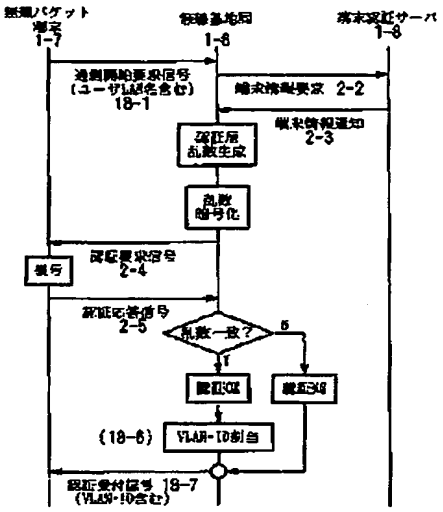
【図１９】

宛先アドレス 4-1	送信元アドレス 4-2	ユーザデータ（暗号化領域） 4-4

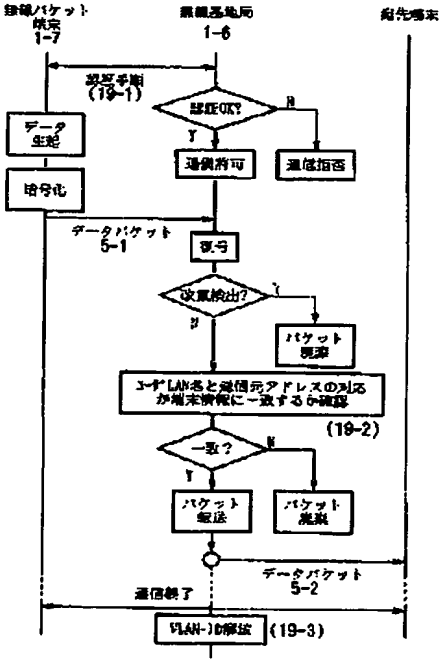
【図１３】



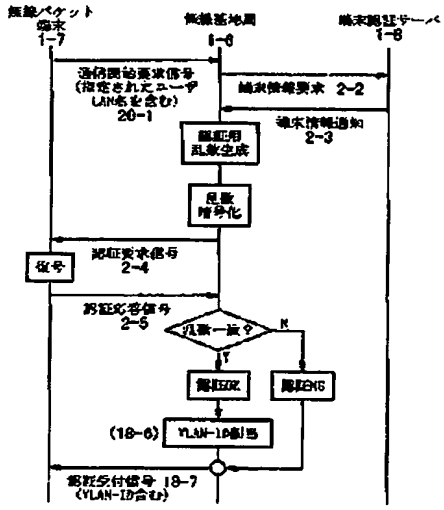
【図１４】



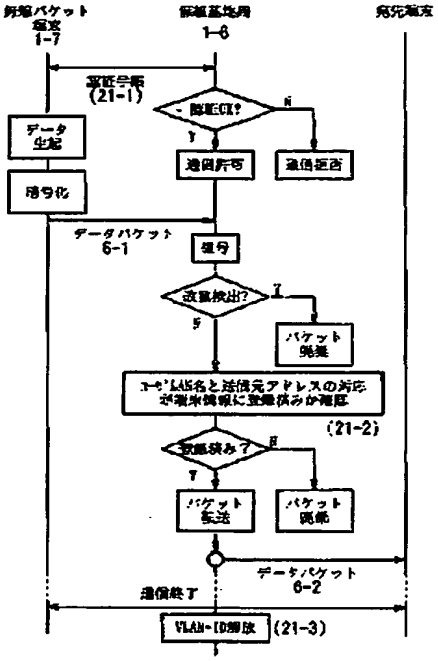
【図１５】



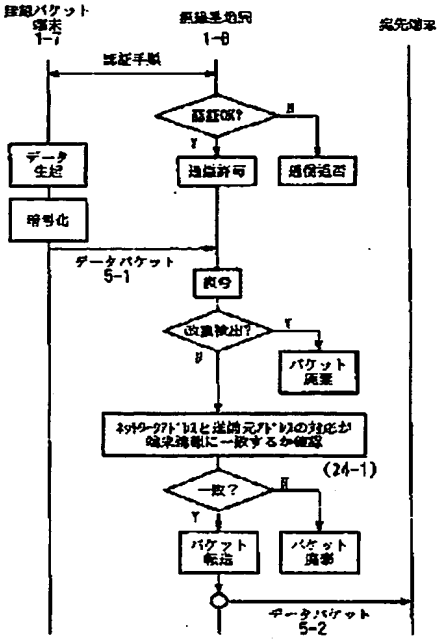
【図１６】



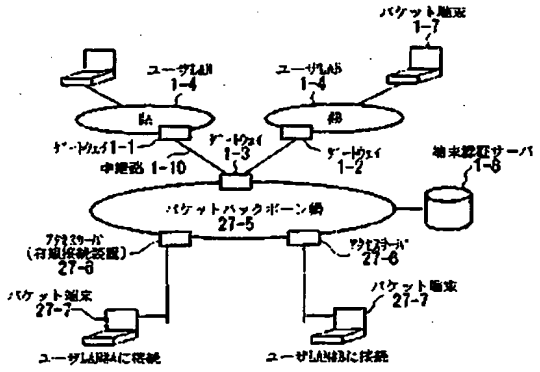
【図１７】


発信パケット端末 1-7
無線基地局 1-8
宛先端末
認証手順 (21-1)
認証OK?
データ生起
通信許可
通信拒否
暗号化
データパケット 6-1
復号
改竄検出?
パケット廃棄
ユーザLAN名と送信元アドレスの対応が端末情報に登録済みか確認 (21-2)
登録済み?
パケット転送
パケット廃棄
データパケット 6-2
通信終了
VLAN-ID解放 (21-3)

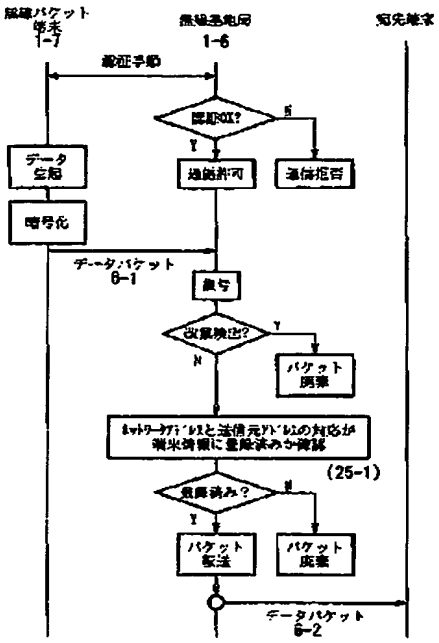
【図２０】


着信パケット端末 1-7
無線基地局 1-8
宛先端末
認証手順
認証OK?
データ生起
通信許可
通信拒否
暗号化
データパケット 5-1
復号
改竄検出?
パケット廃棄
ネットワークアドレスと送信元アドレスの対応が端末情報に一致するか確認 (24-1)
一致?
パケット転送
パケット廃棄
データパケット 5-2

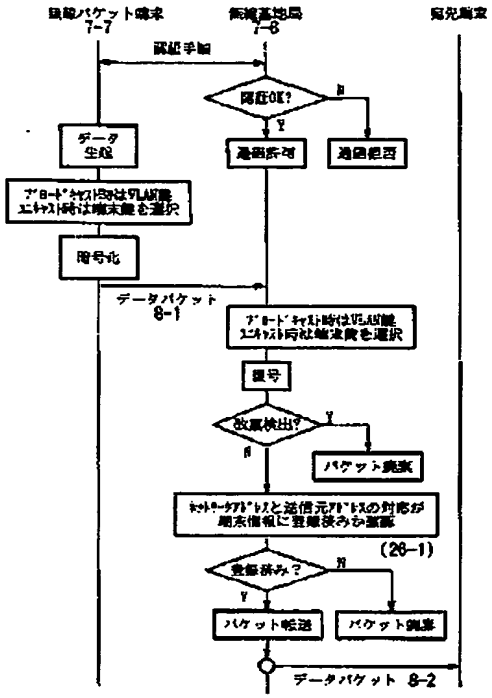
【図２７】


パケット端末 1-7
ユーザLAN 1-4
ユーザLAN 1-4
LAN
LAN
ゲートウェイ 1-1
中継部 1-10
ゲートウェイ 1-3
ゲートウェイ 1-2
端末認証サーバ 1-6
パケットバックボーン網 27-5
アクセスサーバ (有線接続装置) 27-8
アクセスサーバ 27-6
パケット端末 27-7
パケット端末 27-7
ユーザLAN#Aに接続
ユーザLAN#Bに接続

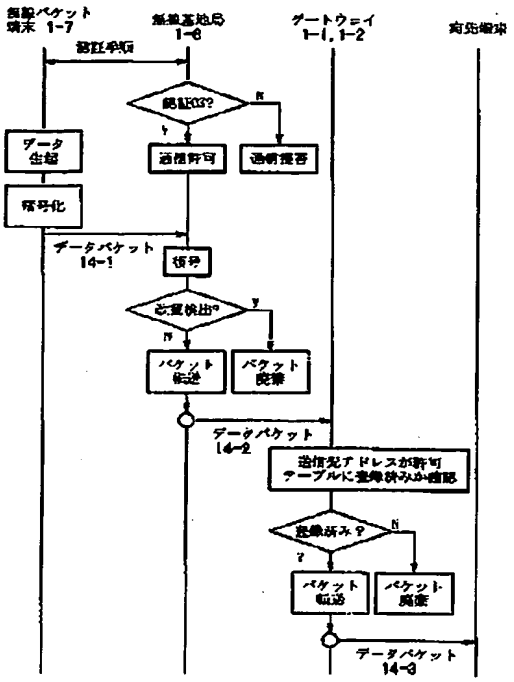
【図２１】


1-7
1-6
認証手順
認証OK?
N
Y
データ生起
通信許可
通信拒否
暗号化
データパケット
6-1
復号
改竄検出?
Y
N
パケット廃棄
(25-1)
登録済み?
N
Y
パケット転送
パケット廃棄
データパケット
6-2

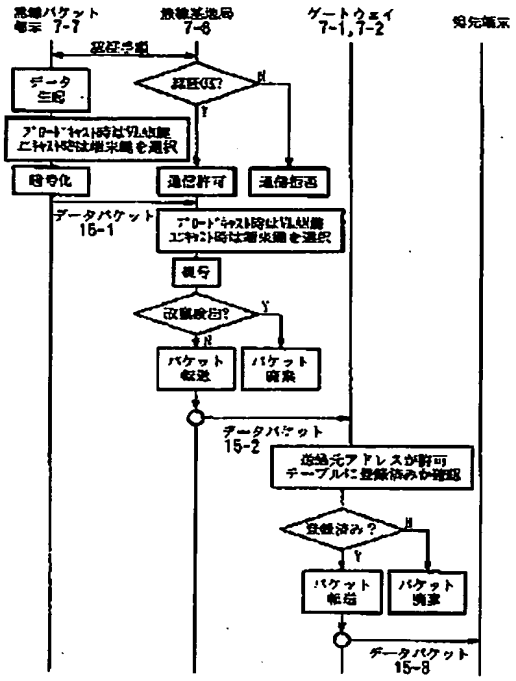
【図２２】


1-7
1-8
認証手順
認証OK?
N
Y
データ生成
通信許可
通信拒否
暗号化
データパケット
8-1
復号
改竄検出?
Y
N
パケット廃棄
(26-1)
登録済み?
N
Y
パケット転送
パケット廃棄
データパケット 8-2

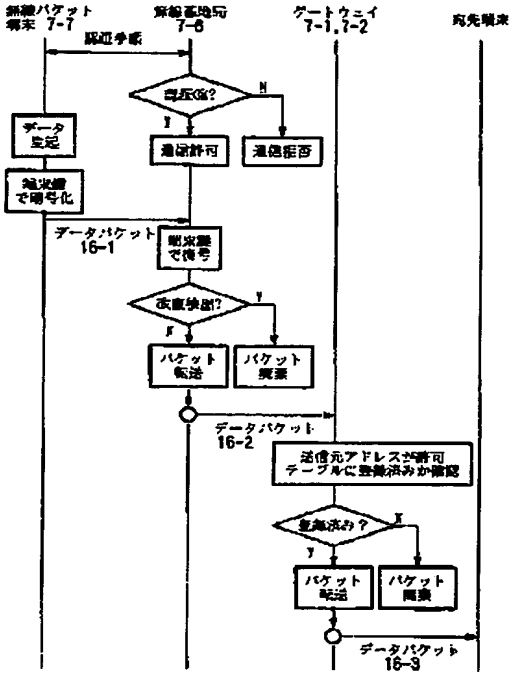
【図２３】


送信端末 1-7
無線基地局 1-8
ゲートウェイ 1-1, 1-2
宛先端末
認証手順
認証OK?
N
Y
通信許可
通信拒否
データ生起
暗号化
データパケット 14-1
宛先
宛先検出?
Y
N
パケット転送
パケット廃棄
データパケット 14-2
送信元アドレスが許可テーブルに登録済みか確認
登録済み?
N
Y
パケット転送
パケット廃棄
データパケット 14-3

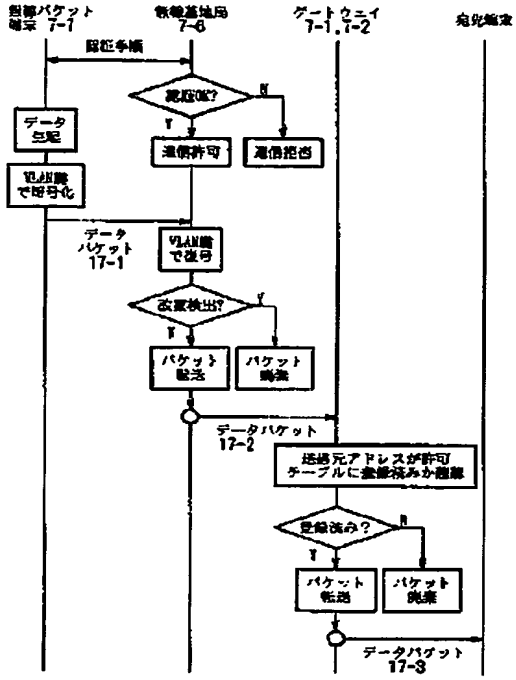
【図２４】


送信端末 7-7
無線基地局 7-8
ゲートウェイ 7-1, 7-2
宛先端末
認証手順
データ生起
認証OK?
N
Y
ブロードキャスト時はVLAN識別子、ユニキャスト時は端末鍵を選択
暗号化
通信許可
通信拒否
データパケット 15-1
ブロードキャスト時はVLAN識別子、ユニキャスト時は端末鍵を選択
宛先
改竄検出?
Y
N
パケット転送
パケット廃棄
データパケット 15-2
送信元アドレスが許可テーブルに登録済みか確認
登録済み?
N
Y
パケット転送
パケット廃棄
データパケット 15-3

【図２５】



【図２６】



フロントページの続き

(72)発明者　畠梨　斉
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　守倉　正博
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内